## Concepts

**CIA**
- **Negative:** (DAD disclosure alteration and destruction)
- Confidentiality: prevent unauthorized disclosure
- Integrity: no unauthorized modifications, consistent data
- Availability: reliable and timely accessible

**Legislative drivers**
- FISMA (federal agencies)
  - Phase 1: categorizing, selecting minimum controls, assessment
  - Phase 2: create national network of secure services to assess
- NIST
  - 8 elements reassessments owners have responsibilities. Benefits: consistent, comparable, repeatable
- OECD
  - Accountability, awareness, ethics, etc. Load of one word things

**Information classification**
- **WHY?** Not all data has the same value, demonstrates business commitment to security, identify which information is most sensitive and vital
- **Criteria:** Value, age, useful life, personal association

### Levels
- Government, military
  - Unclassified
  - Confidential but unclassified (answers to test, healthcare)
  - Confidential (some damage)
  - Secret (Serious damage)
  - Top Secret (Grave damage)

### Private sector
- Public
- Sensitive
- Private
- Confidential

## Controls

**Prime objective** is to reduce the effects of security threats and vulnerabilities to tolerable level

**Risk analysis** process that analyses threat scenarios and produces a representation of the estimated Potential loss

### Types
- Physical, Technical, Administrative

### Standards
- Specify use of specific technologies in a uniform way

### Types
- Regulatory: (required due to laws, regulations)
- Advisory: (not mandatory but strongly suggested)
- Informative: to inform the reader

## Information Security Officer

### Functional responsibility

## Policies

**Policies** first and highest level of documentation

**Very first** is called Senior management Statement of Policy,

- Stating importance, support and commitment

### Types
- Regulatory: (required due to laws, regulations, compliance and specific industry standards)
- Advisory: (not mandatory but strongly suggested)
- Informative: to inform the reader

## Roles and responsibilities

### Security Analyst

#### Strategic, develops policies and guidelines
- Owner
  - Responsible for asset
  - Determine level of classification
  - Review and change classification
  - Can delegate responsibility to data custodian
  - Authorize user privileges
- Custodian
  - Run regular backups/restores and validity of them
  - Insuring data integrity and security (CIA)
  - Maintaining records in accordance to classification
  - Applies user authorization
- End-user
  - Uses information as their job
  - Follow instructions in policies and guidelines
  - Due care (prevent open view by e.g. Clean desk)
  - Use corporation resources for corporation use
- Auditor
  - Examines security controls

## Legislative drivers

**FISMA (federal agencies)**
- Phase 1: categorizing, selecting minimum controls, assessment
- Phase 2: create national network of secure services to assess

## Risk Management

**GOAL**
- Determine impact of the threat and risk of threat occurring

### Activities
- Primary (risk assessment, mitigation methodology)
- Secondary (data collection and sources for risk analysis)

## Types of Risk
- Inherent chance of making an error with no controls in place
- Control: chance that controls in place with prevent, detect or control errors
- Detection: chance that auditors won’t find an error
- Residual: risk remaining after control in place
- Business: concerns about effects of unforeseen circumstances
- Overall: combination of all risks aka Audit risk

## Preliminary Security Examination (PSE)
- Helps to gather the elements that you will need when the actual Risk Analysis takes place.

### Analysis
- Steps: Identify assets, identify threats, and calculate risk.
- **Qualitative HAPPY FACES**
  - Higher level, brainstorming, focus groups etc
- **Quantitative VALUES!!**
  - SLE (single Loss Expectancy) = Asset Value * Exposure factor (% lost of asset)
  - ALE (Annual loss expectancy) = SLE * ARO (Annualized Rate of occurrence)

### Remedies
- Accept, mitigate (reduce by implementing controls)
- Assign (insure the risk to transfer it)
- Avoid (stop business activity)

## Risk Based Audit approach
- Planning and information gathering
- Access internal controls
- Compliancy testing
- Substantive tests
- Finalize the audit
### Controls

**Primary controls**

**Administrative**
- Preventive: hiring policies, screening security awareness (also called soft-measures!)
- Detective: screening behavior, job rotation, review of audit records

**Technical (aka Logical)**
- Preventive: protocols, encryption, biometrics (smartcards, routers, firewalls)
- Detective: IDS and **automatic** generated violation reports, audit logs

**Operational controls**
- Preventive: procedures, training
- Detective: motion detectors, thermal detectors video cameras

**Types**

**Mandatory access control**
Authorization depended on security labels which indicate clearance and classification of objects (Military). Restriction: need to know can apply. Lattice-based is part of it! (A as in mandatory!). Rule-based access control. Objects are: files, directories and devices

**Discretionary access control**
Access through ACL’s. Discretionary access protection (object reuse, protect audit trail). User-directed access control (identity based and hybrid based are also forms of discretionary). Identity Based AC

**Non-discretionary access control**
A central authority determines what subjects have access based on policies. Role-based/task-based. Also lattice based can be applied (greatest lower, least upper bounds apply)

### Something a user knows

- **Passwords**
  - cheap and commonly used
  - password generators
  - user chooses own (do triviality and policy checking)

- **One-time password aka dynamic password**
  - used only once

- **Static password**
  - Same for each logon

- **Passphrase**
  - easiest to remember. Converted to a virtual password by the system.

- **Cognitive password**
  - easy to remember like your mother’s maiden name

### Hacking

- **password checker and password hacker**
  - both programs that can find passwords (checker to see if its compliant, hacker to use it by the hacker)

- **hashing and encryption**
  - On windows system with utility SYSKEY. The hashed passwords will be encrypted in their store LM hash and NT Hash
  - some OS’s use Seed SALT or NONCE, random values added to the encryption process to add more complexity

### Something a user has

- Key, swipe card, access card, badge **PASSWORDS. tokens**

### Static password token

- owner authenticates to token, token authenticates to the information system

**Synchronous (TIME BASED) dynamic**, uses time or a counter between the token and the authentication server, secure-ID is an example

**asynchronous (NOT TIME BASED) server sends a nonce (random value) This goes into token device, encrypts and delivers a one-time password, with an added PIN its strong authentication**

**Challenge/response token**
- generates response on a system/workstation provided challenge
**Something a user is**
- Behavioral
- Physical

**BIOMETRICS**
- Most expensive
- Acceptable 2 minutes per person for enrollment time
- Acceptable 10 people per minute throughput time
- Iris is the same as long as you live
- **Type 1 error:** False rejection rate FRR
- **Type 2 error:** False Acceptance rate FAR
- CER Crossover Error Rate or EER Equal Error rate, where FRR = FAR. The lower CER/EERR the more accurate the system.

**No sunlight in iris scanner**

**What you do:** behavioral authentication, not availability

**What you are:** physical authentication, not availability

**Remote connectivity via dial in** (user dials in to access server, access server prompt for credentials, user enters credentials and forwards to radius server, radius server accepts or rejects). USES UDP. Incorporates an AS and dynamic/static password

**KDC** = Kerberos Distribution Center, grants tickets to client for specific servers. Knows all secret keys of all clients and servers from the network

**TGT** - Ticket granting server

**TGS** - Ticket granting server

**KRB5** - Kerberos (replaced NTLM=NT-LAN Manager)

**Kerberos** is based on symmetric key cryptography (and is not a propriety control)

- Time synchronization is critical
- **MIT project Athena**
- Kerberos is included in windows now
- Replaces NTLM=NT-LAN Manager
- Passwords are never exchanged only hashes of passwords

**Benefits:**
- Inexpensive, loads of OS’s mature protocol
- Smarter than storage cards

**RADIUS**
- Works with PACS (Privileged Attribute Certificates)
- Sesame uses both symmetric as asymmetric encryption (thus improvement upon Kerberos)

**KRYPTOKNIGHT**
- IBM – thus RACF
- Peer-to-peer relationship between KDC and parties

**SECURITY**
- Scripting scripts contain logon information that authenticates users
- **DIRECTORY SERVICE**
  - Hierarchical naming schema
  - Active directory has sophisticated security resources (group policy, user rights accounts, DNS services)

**Decentralized access control**

**Database**
- Relation: basis of the database consists of a two dimensional table
- ROWS are records of tuples. Number of rows is cardinality
- **Columns** are attributes. Number of columns is the degree

**Primary Key**
- Unique identifier in a table

**Foreign Keys**
- Foreign Keys: used to enforce relationship between two tables. This is also called referential integrity, that you don’t have a nonexistent reference.

**Smart Cards**
- **IEC 14443 = smartcards**
- The combi-card – also known as a dual-interface card – has one smart chip embedded in the card that can be accessed through either contact pads or an embedded antenna.
  - Smarter than storage cards
  - Storage smart card holds RSA key pairs in memory
  - RSA smart cards have processor that compute (sign and verify RSA certificates) and create RSA key pairs
**Identity management**
Performs all of IAAA

**Directory based**
- hierarchical x500 standard protocol like LDAP for allowing subjects to interact with the directory
- Organized through name spaces (Through Distinguished names)
- Needs client software to interact
- META directory gathers information from multiple sources and stores them into once central directory and synchronizes
- VIRTUAL directory only points where the data resides

**Web Access Management**
- allows administrators to control what users can access when browsing enterprise assets
- mostly working as stateless HTTP, during session you are authenticated, once logged of you have to re-identify and authenticate
- Can also work as Single Sign on by use of SSL where through the use of COOKIES the authentication is being held in memory (preferably) or text file

**Password Management**
- Password Synchronization. Systems synchronize the passwords to multiple systems. User has one password but has to re-authenticate at every system. Danger: if one password is hacked, all resources can be accessed. Differs from legacy sign on: Users authenticate once then will gain access without re-authentication
- Self-Service password reset. Personal questions (pet’s name, mother’s maiden name). Often done by question, then sending mail with link so identity tied to the answer
- Assisted password reset. Help Desk authenticates you by question and answer

**Account management**
- life cycle management (creating, modifying and deleting accounts)
- Can be automatically or by tickets for technical administrators on request of the managers
- mainly for internal accounts

**Provisioning**
- user information taken from HR (authoritative source)
- Identity data put in an centralized directory (identity repository)
- manager will appoint new employees, accounts are created automatically
- user provisioning refers to creation, maintenance and deactivation of user objects and attributes on systems, directories or application in response to business processes.

**Profile update**
- collection of data associated with identity is called a profile
- self service is it called when a user can update his own non-sensitive data
- digital entity is made up of different attributes (like manager, sex height etc) has clearance level yyy etc
- Federation = sharing identity and authentication behind the scenes (like booking flight -> booking hotel without re authenticating) by using a federate identity so used across business boundaries

**Network security**
NIST 800-42 = security testing
War driving: driving a car with notebook to find open access point to a network

**IDS intrusion detection system**
**NETWORK BASED**
- Detects intrusions on the local area network behind a firewall.
- Is passive while it acquires data.
- Reviews packets and headers
- Problem with network based is that it will not detect attacks by users logged into hosts

**HOST BASED**
- monitoring servers through EVENT LOGS AND SYSTEM LOGS
- as good as the completeness of the host logging

**Signature based method (AKA Knowledge based):** compared with signature attack database (aka misuse detector)
Statistical anomaly based: defines a ‘normal’ behavior and detects abnormal behaviors.

Response box is a part of an IDS that initiates alarm or activity

**Components:** Information source/sensor, centralized monitor software, data and even report analysis, database components and response to an event or intrusion

**IPS Intrusion prevention system**
Detect attack and PREVENT that attack being successful

**Penetration testing**
- Blue team had knowledge of the organization, can be done frequent and least expensive
- Red team is external and stealth
- White box ethical hacker knows what to look for
- Black box ethical hacker not knowing what to find

4 stages: planning, discovery, attack, reporting
vulnerabilities exploited: kernel flaws, buffer overflows, symbolic links, file descriptor attacks
other model: footprint network (information gathering) port scans, vulnerability mapping, exploitation, report scanning tools are used in penetration tests flaw hypotheses methodology = operation system penetration testing

**Other things to know**
Constrained user interfaces limit the functions that can be selected by a user
threat: something that could happen to a system, vulnerability: is a weakness or hole in the security

Race Condition: when two or more processes use the same resource and the sequence of steps within the software can be carried out in an improper order, thus like force the authorization step to take place before the authentication step.

TOC/TOU Attack is an asynchronous attack when an attacker interrupts a task and changes something to affect the result

The system key (SYSKEY) protects security information (including password information) in the Active Directory database and other Local Security Authority (LSA) secrets against offline attacks by encrypting their storage on a domain controller in a Windows server

Hardening an operation system: disable services and remove unnecessary applications
allowing downloads on a honey pot = illegal (entrapment)
Categories within a security label are used to enforce need to know fault generation = getting the encryption key
Network Availability

Raid levels
RAID 0 Striped, one large disk out of several –Improved performance but no fault tolerance
RAID 1 Mirrored drives –fault tolerance from disk errors and single disk failure, expensive
RAID 2 not used commercially. Hammond Code Parity
RAID 3 Striped on byte level with extra parity drive –Improved performance and fault tolerance, but parity drive is a single point of failure and write intensive.
RAID4 Same as Raid 3 but striped on block level
RAID 5 Striped on block level, parity distributed over all drives –requires all drives but one to be present to operate hot-swappable. Interleave parity
RAID 6 Dual Parity, parity distributed over all drives –requires all drives but two to be present to operate hot-swappable
RAID 7 is as raid5 but all drives act as one single virtual disk
0+1 –striped sets in a mirrored set (minimum four disks; even number of disks)

Server fault Tolerant Systems
Redundant servers – applies raid 1 mirroring concept to servers. On error servers can do a fail-over. This AKA server fault tolerance
Server clustering – group of independent servers with are managed as a single system. All servers are online and take part in processing service requests. On error on a server only performance is affected.AKA server farm

Single point of failures
Cabling
Twisted pair to long, Cat 5 better than cat3 for interference
Fiber optics immune to EMI, can be broken and high-cost/expertise
Topoology failures
Ethernet twisted pair more resistant than coaxial
Token Ring because a token is passed by every station, a NIC that’s is set to wrong speed or error can take all network down
Fiber Distributed Data Interface form of token ring that has second ring that activates on error
Leased lines use multiple lines and/or multiple vendors
Frame Relay WAN over a public switched network. High Fault tolerance by relaying fault segments to working.

Network abuse
Class A: unauthorized access by circumventing access controls. Legitimate users that gain higher access or pretends to be another user (masquerading)
Class B – unauthorized use of network for non business properties
Surfing internet, porn sites, private emails
Class C – Eavesdropping
Interception of network traffic. Tapping = physical interception like clipping
Passive eavesdropping: monitoring or listening to transmissions
Active eavesdropping: tampering with an transmission to create covert channels or actively probing the network
Class D – Denial of service or other service disruptions (see under network attacks)

Network attacks – Denial of Service
Used to overwhelm a targets resources
- Filling up hard drive by using huge email attachments or file transfers
- Sends messages to reset targets host subnets masks
- Using up all system resources

DOS - performed by sending malformed packets to a system; can interrupt service or completely deny legitimate users of system resources
DDOS – botnet, zombie, massive dos attack using multiple computers

SMURF – ICMP requires three players (attacker, victim and amplifying network); attacker spoofs packet header to make it appear that it originated on the victim system with amplifying network broadcasting the message.
Countermeasures – disable broadcast at border routers; border routers should not accept packets that originate within network; restrict ICMP traffic (Hint IC = Its Smurf though spelled wrong)

FRAGGLE – similar to Smurf but uses UDP
Countermeasures – disable broadcast at border routers; border routers should not accept packets that originate within network; restrict UDP traffic; employ IDS, apply appropriate patches.

Land Attack - The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address and an open port as both source and destination. The reason a LAND attack works is because the machine to reply to itself continuously.

SYN FLOOD - TCP packets requesting a connection (SYN bit set) are sent to the target network with a spoofed source address. The target responds with a SYN-ACK packet, but the spoofed source never replies. This can quickly overwhelm a system’s resources while waiting for the half-open connections to time out. This causes the system to crash or otherwise become unusable. Counter: sync cookies/proxies, where connections are created later

Teardrop - The length and fragmentation offset fields of sequential IP packets are modified, causing the target system to become confused and crash.

Common Session Hijacking Attacks:

Session hijacking (Spoofing) - IP spoofing involves altering a TCP packet so that it appears to be coming from a known, trusted source, thus giving the attacker access to the network.

TCP sequence number attack – intruder tricks target to believe it is connected to a trusted host and then hijacks the session by predicting the targets choice of an initial TCP sequence number
**Network layers OSI MODEL**

(Latter succeeded by TCP/IP)

**HINT:** All People Seems to Need Data Processing

It encapsulates data when going through the layers

**Application – layer 7 – C, AU, I, NR**

FTP, SMB, TELNET, TFTP, SMTP, HTTP, NNTP, CDP, Gopher, SNMP, NDS, AFP, SAP, NCP, SET. Technology: Gateways. **User data**

**Presentation – layer 6 – C, AU, Encryption**

Translations like EBCDIC/ANSI; compression/decompression and encryption/decryption. Standards like JPEG, TIFF, MID. Technology: Gateway. **Messages**

**Session -layer 5 – None**

Inter-host communication, simplex, half duplex, full duplex. Protocols as NSF, SQL, RADIUS, and RPC. Technology: Gateway

**Transport – layer 4 – C, AU, I**

End-to-end data transfer services and reliability. Technology: Gateways. **Datagrams**

Protocols: TCP, UDP, SSL, SSH-2, SPX, NetBIOS, ATP

**Network – layer 3 – C, AU, I**

Path selection and logical addressing. Technology: Virtual circuits (ATM), routers. **Packets**

Message routing, error detection and control of node data are managed. IP, IPSEC, ICMP, BGP, OSPF, RIP, BOOTP, DHCP, ZIP, DDP, X.25 and IGMP

**Data Link – layer 2 - C**

This layer deals with addressing physical hardware. Translates data into bits and formats them into data frames with destination header and source address. Error detection via checksums.

LLC: the Logical Link Control Sub layer. Flow control and error notification.

MAC: the Media Access Control layer. Physical addressing. Concerns frames, logical topologies and MAC-addresses.


**Physical – layer 1 - C**

Converts bits into voltages or light impulses. Hardware and software drivers are on this level. It sends and receives bits. Physical topologies: BUS, MESH, STAR, TREE, RING

**Network layers TCP/IP Model**

Developed by Department of Defense in the 1970s to support the construction of the internet

**HINT:** AHIN

**Application – layer 4 (Application/Presentation/Session)**

Applications and processes that uses the network

**Host-to-Host – Layer 3 (Transport)**

End-to-end data delivery

Protocols: TCP and UDP

**Internet – Layer 2 (corresponds to OSI network layer)**

Defines the IP datagram and handles routing of data across networks

Protocols: IP, ARP, RARP, ICMP

**Network access – Layer 1 (Data link, Physical)**

Routines for accessing physical networks and the electrical connection

**Network Protocols**

**Transmission control protocol TCP** – reliable, sequences and works with acknowledgements. Provides a manageable data flow to avoid congestions overloading and data loss. (like having a telephone conversation with someone). Connection Oriented.

**User datagram protocol UDP** – unreliable, scaled down version of TCP, no error correction, no sequencing. Less overhead. (like sending a letter to someone). Connectionless.

**Internet protocol IP** all hosts have an IP address. Each data packet has an IP address of sender and recipient. Routing in network is based upon these addresses. Considered unreliable datagram service because there’s no guarantee that the packet will be delivered, not even that its delivered only once and no guarantee that its delivered in the same sequence that its sent. 32 bits long, IPv6 is 128 bits long

**Address resolution protocol ARP:** Used to match an IP address to a hardware MAC address. ARP sends out broadcast to a network node to reply with its hardware address. It stores the address in a dynamic table for the duration of the session, so ARP requests are only sent the first time

**Reverse address resolution protocol RARP:** When a hardware address is known but the IP address has to be found. (like an diskless machine)

**Internet control message protocol ICMP:** sends messages between network nodes regarding the health of the network. Also informs about rerouting incase of errors. Utility PING uses ICMP messages to check physical connectivity of the network machines

**Telnet** terminal emulation enables user to access resources on another machine. Port 23

**File Transfer Protocol FTP** for file transfers. Cannot execute remote files as programs. Authentication. Port 20 and 21

**Trivial File Transfer Protocol TFTP** stripped down, can only send/receive but not browse directories. No authentication thus insecure. Port 69

**Network File System NFS** protocol that supports file sharing between two different file systems

**Simple Mail Transfer protocol SMTP** email queuing. Port 25

**Line printer daemon LPD** for printing and spooling

**X Windows** graphical user interface

**Simple Networking Management Protocol SNMP** collection of network information by polling the devices from a management station. Sends out alerts –called traps- to an database called Management Information Bases (MIBs)

**Bootstrap Protocol BootP** when wireless workstation is on-lined it sends out a BootP request with its MAC address to get an IP address and the file from which it should boot. Replaced by DHCP

**DHCP:** Dynamic Host Configuration Protocol

**Security Enhancement Protocols**

**TELNET:** Remote terminal access and Secure Telnet

**REMOTE PROCEDURE CALL:** Secure remote procedure call (SRA)

**Security Focused Protocols**

At application layer of OSI:

**Secure Electronic Transaction (SET)** authentication for credit card transactions. Overtaken by SSL

**Secure HTTP S-HTTP** encrypting HTTP documents. Also overtaken by SSL

At Transport layer of OSI:

**Secure Shell (SSH-2)** Authentication, compression, confidentiality and integrity.

Uses RSA certificates for authentication and triple DES for encryption

**Secure Socket Layer (SSL)** encryption technology to provide secure transactions like credit card numbers exchange. Two layered: SSL record protocol and handshake protocol. Same as SSH it uses symmetric encryption for private connections and asymmetric or public key cryptography for peer authentication. Also uses message authentication code for integrity checking.

**Simple Key Management for Internet Protocols (SKIP)** provides high availability in encrypted sessions to protect against crashes. Exchanges keys on a session by session basis.
Virtual Private Networks (VPN)

A VPN is created by dynamically building a secure communications link between two nodes using a secret encapsulation method via network address translation (NAT) where internal IP addresses are translated to external IP addresses.

VPN Protocols

Hint: TP at end for Tunneling Protocols

- Point to Point tunneling protocol (PPTP)
  - Works at data link layer of OSI
  - Only one single point-to-point connection per session
  - Point To Point protocol (PPP) for authentication and tunneling
  - Dial-up network use

Layer 2 tunneling protocol (L2TP)

- Also in data-link layer of OSI
- Single point-to-link connection per session
- Dial-up network use
- Port 115

IPSEC

- Operates at Network Layer of OSI
- Enables multiple and simultaneous tunnels
- Encrypt and authenticate
- Build into IPv6
- Network-to-network use

VPN Devices

Is hard- or software to create secure tunnels

IP-ssec compatible

- Encryption via Tunnel mode (entire data package encrypted) or Transport mode (only datagram encrypted)
- Only works with IP at Network layer of OSI

NON IP-ssec compatible

Socks-based proxy servers Used to reach the internal network from the outside. Also contains strong encryption and authentication methods

PTP used in windows machines. Multiprotocol, uses PAP or CHAP

Dial-up VPN’s remote access servers using PPTP commonly used by ISP’s

Secure Shell SSH2 not strictly a VPN product but opens a secure encrypted shell session from the internet through a firewall to a SSH server

DATA NETWORK TYPES

Local Area Network (LAN)

Limited geographically to e.g. a building. Devices are sharing resources like printers, email and files. Connected through copper wire or fiber optics.

CAN: campus area network, multiple building connected to fast backbone on a campus

MAN: metropolitan network extends over cities

Wide Area Network (WAN)

Connects LANS over a large geographical area

Internet intranet and extranet

Internet is global, intranet local for use within companies and extranet can be used e.g. by your customers and clients but is not public.

DATA NETWORK SIGNALS

Analog signal

Infinite wave form, continuous signal, varied by amplification

Digital signal

Saw-tooth form, on-off only

Asynchronous sends bits of data sequentially. Same speed on both sides. Modems and dial-up remote access systems

Synchronous very high speed governed by electronic clock timing signals

LAN Cables

Twisted pair

Shielded (STP) or unshielded (UTP) Cat 3=10BaseT, Cat5=100BaseT

Coaxial

More EMI resistant. Baseband: only one single channel, Broadband: multiple signal types like data, video, audio

Fiber Optic

Most expensive, but hard to tap and resistant to EMI

LAN Transmission Protocols

Carrier Sense Multiple Access (CSMA) for Ethernet. Workstations send out packet. If it doesn’t get an acknowledgement it resends

CSMA with Collision Avoidance (CSMA/CA) is attached by 2 coax cables. In one direction only. Wireless 802.11

CSMA with Collision Detection (CSMA/CD) only one host can send at the time, using jamming signals for the rest

Polling Host can only transmit when he polls a secondary to see if it’s free

Remote access servers using PPTP commonly used by ISP’s

Secure Shell SSH2 not strictly a VPN product but opens a secure encrypted shell session from the internet through a firewall to a SSH server
### WAN Protocols

#### Private Circuit technologies

- **Dedicated line** reserved communication, always available
  - T1, 1.5 Mbps through telephone line
  - T3, 44.7 Mbps through telephone line
  - E1 European 2048 Mbps digital transmission

#### Leased line

- can be reserved for communications.
- Type of Dedicated line.

#### X.25

- Defines point-to-point communication between Data terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE)
- LAPB was created for use with X.25.
- LAPB defines frame types and is capable of retransmitting, exchanging and acknowledging frames as detecting out-of-sequence or missing frames.

#### Frame Relay

- High performance WAN protocol designed for use across ISDN interfaces. Is fast but has no error correction.

#### Switched Multimegabit Data Service (SMDS)

- High speed communication over public switches networks for exchanging ‘bursts of data’ between enterprises

#### Asynchronous Transfer mode (ATM)

- Very high bandwidth. It uses 53-byte fixed size cells instead of frames like Ethernet. It can allocate bandwidth up on demand making it a solution for Bussy applications. Requires fiber optics.

#### Voice over IP (VOIP)

- Combines many types of data into a single IP packet. Cost, interoperability and performance wise it’s a major benefit.

### Other important WLAN protocols

#### Synchronous Data Link Control (SDLC)

- Created by IBM for mainframes to connect to their remote offices. Uses a polling media access method. Works with dedicated leased lines permanently.

#### Data Link layer of OSI model

- Data link layer of OSI model.

#### High-level Data Link Control (HDLC)

- Extension to SDLC also for mainframes. Uses data encapsulation on synchronous serial links using frame characters and checksums. Also data link layer.

#### High Speed Serial Interface (HSSI)

- Digital signals. Data link layer.

#### Fiber Distributed Data Interface (FDDI)

- Token passing dual token ring with fiber optic. Long distances, minimal EMI interference.

#### Fiber Distributed Data Interface (FDDI)

- Arcnet uses a token –passing in a star technology on coax

#### Fiber Distributed Data Interface (FDDI)

- IBM created. All end stations are connected to a MAU Multi Access Unit. CAU: Controlled Access Units – for filtering allowed MAC addresses.

#### Fiber Distributed Data Interface (FDDI)

- Fiber Distributed Data Interface (FDDI) token-passing dual token ring with fiber optic. Long distances, minimal EMI interference.

#### Fiber Distributed Data Interface (FDDI)

- Allows several tokens at the time active

### LAN Devices

#### Repeaters

- Amplify data signals to extend range (physical)

#### HUBS

- Connect multiple LAN devices into a concentrator. Is actually a multi-port repeater (physical)

#### Bridges

- Forward data to all other network segments if it’s not on the local segment. Operates at level 2 (thus no IP-addressing here)

#### Routers

- Opens up data packet, reads hardware or network address and then forwards it to the correct network

#### Gateway

- Software that acts as access point to another network or device that translates between different protocols

#### LAN extenders

- Remote access, multi layer switch that connects LANs over a WAN

### LAN Transmission Methods

#### Unicast

- Packet is send from single source to single destination

#### Multicast

- Source packet is copied and send to multiple destinations

#### Broadcast

- Source packet is copied and send to all nodes

### LAN Topologies

#### BUS

- All transmissions have to travel the full length of the cable

#### RING

- Workstations are connected to form a closed loop

#### TREE

- Bus type with multiple branches

#### MESH

- All nodes interconnected

### LAN Media Access

#### Ethernet IEEE 802.3

- Using CSMA with a BUS-topology

#### Thinnet:

- 10base2 with coax cables up to 185 meters

#### Thicknet:

- 10Base5, coax up to 500 meters

#### UTP:

- 10BaseT=10Mbps
- 100BaseT=Fast Ethernet =100Mbps
- 1000BaseT=Gigabit Ethernet=1Gbps

#### Ethernet networks were traditionally designed to work with more sporadic traffic than token ring networks

### Domain 3 – Telecommunications and Networks
Remote Access Technologies

Asynchronous Dial-Up Access
This is how everyone connects to the internet. Using a public switched telephone network to access an ISP

Integrated Serviced Digital Network (ISDN)
communication protocol that permits telephone line to carry data, voice and other source traffic. Two types: BRI Basic rate interface and Primary Rate Interface (PRI)

xDSL
uses regular telephone lines for high speed digital access

Cable Modems
Via single shared coaxial cable, insecure because of not being filtered or firewalled

Remote Access Security Technologies

Restricted Address
incoming calls are only allowed from specific addresses on an approval list. This authenticates the node, not the user!

Callback
User initiates a connection, supplies identifying code, and then the system will call back a predetermined telephone number. Also less useful for travelling users

Caller ID
checks incoming telephone number against an approval list and then uses Callback. Less useful for travelling users.

Remote Node Security Protocols

Password Authenticate Protocol PAP
Provides identification and authentication of the user using static replayable passwords. No encryption of user-id or password during communication

Challenge Handshake Authenticate Protocol (CHAP)
non-replayable challenge/response dialog

Remote Access Authentication Systems

Terminal Access Controller Access Control System TACACS
User passwords are administered in a central database instead of individual routers. A network device prompts user for a username and static password then the device queries a TACACS server to verify the password. TACACS does not support prompting for password change or use of dynamic password tokens. Port 49

TACACS+
Enhanced version with use of two factor authentication, ability to change user password, ability of security tokens to be resynchronized and better audit trails and session accounting

Remote Authentication Dial-In User Service RADIUS
Often uses as stepping stone to the more robust TACACS+. Clients sends their authentication request to a central radius server that contains all of the user authentication and network ACL’s. RADIUS does not provide two way authentication, therefore it’s not used for router-to-router authentication. Port 1812. Contains dynamic password and network service access information (Network ACLs)

Remote Authentication Dial-In User Service RADIUS
Often uses as stepping stone to the more robust TACACS+. Clients sends their authentication request to a central radius server that contains all of the user authentication and network ACL’s. RADIUS does not provide two way authentication, therefore it’s not used for router-to-router authentication. Port 1812. Contains dynamic password and network service access information (Network ACLs)

Things to know

TCP/IP Classes
Class A network number values begin at 1 and end at 127
Class B network number values begin at 128 and end at 191
Class C network number values begin at 192 and end at 223

ISDN
BRI B-channel 64Kbps, D-channel 16Kbps
PRI B- and D-channels are 64Kbps

80211 has CSMA/CA as protocol. Can use DSSS and FHSS (ss stands for spread spectrum)
802.11b uses only DSSS

Before a computer can communicate with the internet, it needs an IP-address, a default gateway and a subnet mask

To connect multiple LAN segments you can use Bridges, Switches and Routers

Fast Ethernet 100Base-TX has as characteristics: 100Mbps data transmission, 1 pairs Cat5 UTP and max segment of 100 meters (328 feet)

Unsubnetted netmask is shown as /24

Other word for DMZ is screened subnet

FTP, RLOGIN and TELNET never uses UDP but TCP

Attenuation is decrease in amplitude as a signal propagates along a transmission medium

SSL session key length is from 40bit to 256 bit

The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Data backups addresses availability, integrity and recovery but not confidentiality

IP headers contain 32-bit addresses (in IPv4) and 128 in IPv6. In an Ethernet local area network, however, addresses for attached devices are 48 bits long.

Wireless

802.11: 1 or 2 mbps, 2.4Ghz, FHSS or DSSS
802.11b: 11 mbps, only DSSS
802.11a:  54 mbps, 5 GHz, Orthogonal Frequency Division
802.11g: 20-54mbps, 2.4GHz
802.11e: QoS
802.16: IEEE 802 Broadband Wireless Access (802 WBA)
802.11i: AES, CCMP, 802.1X authentication.
802.11n: 100mbps, 2.4GHz
**History**

Hieroglyphs - sacred carvings
Scyphile: wound papyrus around a wooden rod to see message
Substitution character: shifting 3 character (C3) for example in the one (mono-alphabet) alphabet system
Cipher disks: 2 rotating disks with an alphabet around it
Jefferson disks: 26 disks that cipher text using a alignment bar
Unix uses rot 13, rotate 13 places in the alphabet
Hagelin machine (M-209) mechanical cryptographic machine

**Symmetric key AKA private key or same key encrypt.**
- Both the receiver and the sender share a common secret key
- Larger key size is safer > 128
- Can be time-stamped (to counter replay attacks)
- Does not provide mechanisms for authentication and non-repudiation

**DES (data Encryption Standard) comes from IBM**
- DEA Data Encryption Algorithm x3.92, using 64 block size and 56bit key with 8bits parity
- 16-rounds of substitution and transposition cryptosystem
- Adds confusion(conceals statistical connect between cipher text and plaintext) and Diffusion (spread the influence of plaintext characters over many cipher text characters by means of transposition like HIDE-> IHED)
- Triple des = three times encrypted DES, preferably with 3 different keys = DES-EE3. Actual key length = 168 bits. Uses 48 rounds of computations (3x16)
- Replaced by AES Advanced Encryption Standard

**Asymmetric key AKA Public Key Encryption**
- Sender and receiver have public and private keys.
- Public to encrypt a message, private to decrypt
- Slower than symmetric, secret key (100 to 1000)

**Public Key Algorithms**
- RSA (Rivest, Shamir and Adelman) works with one way math with large prime numbers (aka trap door functions). Can be used for encryption, key exchange and digital signatures)
- Diffie Hellman Key exchange, about exchanging secret keys over an insecure medium without exposing the keys
- el Gamal, works with discrete logarithms, based on Diffie Hellmann
- DSA Digital Signature Algorithm, the US government equivalent of the RSA algorithm
- ECC - Elliptic Curve Cryptosystem - mathematical properties of elliptic curves, IT REQUIRES FEWER RESOURCES THAN RSA. Used in low power systems (mobile phones etc)

**Digital signatures**
- no modifications allowed
- identity can be derived
  works with a one-way hash (message digest), like SHA-1 (512 bit blocks) or MD5 (128 bits digest) or HMAC that uses a key

**Hybrid systems**
- uses both asymmetrical and symmetrical encryption
  - asymmetrical for key exchange
  - symmetrical for the bulk - thus it is fast
- example: SSL, PGP, IPSEC S/MIME

**PKI**
X.509 standard = PKI
Integrity (hash code and message digest), access control, confidentiality (by encryption), authentication (digital certificates) and non-repudiation (digital signatures)
</p>

**escrowed encryption standard**
- legal monitoring of encrypted transmissions
- divide key into 2 parts, store separately with two trusted organizations
- part of hardware: US Government Clipper Chip with Skipjack Secret Key algorithm; but its 80-bits and weak
- Fair Cryptosystems , each portion of a distributed private key can be verified as correct

**email security**
S/Mime Confidentiality (encryption) Integrity (using PKCS X.509 PKI) and non-rep through signed message digests

**Message Security protocol Military X.400. Sign, Encrypt, Hash**
Pretty Good Privacy, uses IDEA and RSA instead of an CA they use Web of Trust between the people using it
### Domain 4 - Cryptography

**Internet Security**
- Message Authentication Code (MAC) or Financial Institution Message Authentication Standard (FIMAS)
- MACs checks value like CRC

**SET Secure Electronic Transaction**
- Uses DES for encrypting payment information for credit card companies. Covers end to end transactions with digital signatures and digital certificates

**SSL / TLS**
- Netscape!
- Operates at the TRANSPORT layer
- Uses des, idea, 3des and md5 hash x.509 PKI certificates
- does not offer end to end transactions based on sessions
- 40 or 128 bits

**HTTPS**
- running http over SSL, encrypts message and connection

**SHTTP**
- Protects only individual message between computers

**secure Shell (SSH-2)**
- Remote access to network using encrypted tunnels

**WAP**
- class 1: anonymous authentication
- class 2: server authentication
- class 3: two way client server authentication

**WEP**
- Initialization vector, RC4 and symmetric = old do not use

**IOTP**
- Internet Open trading Protocol
  - user chooses payment method and thus encryption

**MONDEX**
- Cash smart card application

**IPSEC**
- 2 protocols: AH Authentication header and ESP Encapsulated Security Payload
- works with Security Associations (SA)’s
- works with IKE protocols
- IKE IS FOR MANAGING SECURITY ASSOCIATIONS
- 2 modes:
  - transport, data is encrypted header is not tunneled
  - new uses rc6; IP header is added, old IP header and data is encrypted

**Definitions**
- **Purpose**: protect transmitted information from being read and understood expect the intended recipient

**Block Cipher**
- segregating plaintext into blocks and applying identical encryption algorithm and key

**Cipher**
- cryptographically transformation that operates on characters or bits

**Cipher text or Cryptogram**: unintelligible message

**Clustering**
- situation wherein plain text messages generates identical cipher text messages using the same algorithm but with different crypto-variables or keys

**Codes**
- cryptographic transformation that operates at the level of words or phrases

**Cryptanalysis**
- breaking the cipher text,

**Cryptographic Algorithm**
- Step by step procedure to encipher plaintext and decipher cipher text

**Cryptography**
- the art and science of hiding the meaning of communications from unintended recipients. (Greek: kryptos=hidden, graphein=to write)

**Cryptology**
- cryptography + cryptanalysis

**Cryptosystem**
- set of transformations from a message space to cipher space

**Decipher**
- To make the message readable, undo encipherment process

**Encipher**
- make message unintelligible

**End-to-end encryption**
- Encrypted information that is sent from point of origin to destination. In symmetric encryption this means both having the same identical key for the session

**Exclusive OR**
- Boolean operation that performs binary addition

**Key or Crypto variable**
- Information or sequence that controls the enciphering and deciphering of messages

**Link encryption**
- stacked encryption using different keys to encrypt each time

**One Time Pad**
- encipher each character with its own unique key that is used only once

**Plaintext**
- message in clear text readable form

**Steganography**
- secret communications where the existence of a message is hidden (inside images for example)

**Work Function (factor)**
- the difficulty of obtaining the clear text form the cipher text as measured by cost/time

**3 states of information**
- data at rest (storage)
- data in transit (the network)
- data being processed (must be decrypted)

**Cipher types**
- block (padding to blocks of fixed size) like DES
- 3DES, AES or stream (bit/byte one by one no padding) like RC4

**Chameleon, leviathan, Sober**

**Things to know**
- skip is a distribution protocol
- RC4 is a stream cipher
- rc5 and rc6 are block cipher
- FIPS 140 hardware and software requirements
- Hash algorithms are also called Message Digests.
- Most used are MD5 (message Digest 128 bits) and SHA1 (signature hashing algorithm 160 bits)
- CRL’s of a PKI environment holds serial numbers
- SHA1 was designed by NIST and NSA to be used in digital signatures
- A root Certificate Authority (CA) must certify its own public key pair
- cross certification does not check authenticity off the certificates in the certificates path
- Traffic analysis: inference of information from analysis of traffic
- Traffic padding: generation of spurious data units
- Collision: Same message digest as a result of hashing.

**Cryptographic Attacks**
- Ciphertext Only: attacker sees only the ciphertext
- Known Plaintext: attacker knows both cipher and plaintext
- Chosen Plaintext: offline attack (attacker prepares list of plaintexts) online attack (attacker chooses the plaintext based on the ciphertext already received)
- Chosen ciphertext: attacker chooses both the plaintext values and the ciphertext values
- Birthday Attack: Collisions appear much fasters.
Protection mechanisms

Protection domain
Execution and memory space assigned to each process

TRUSTED COMPUTER BASE
Combination of protection systems within a computer system, which include the hardware, software and firmware that are trusted to enforce the security policy.

Security Kernel is hardware, software, firmware, elements of TCB that implement the reference monitor concept — must be isolated from reference monitor (reference monitor: isolation, completeness and verifiability, that compares the security labels of subjects and objects)

Protection rings (MIT’s MULTICS design)
Ring 0 - Operating system kernel. The OS’ core. The kernel manages the hardware (for example, processor cycles and memory) and supplies fundamental services that the hardware does not provide.
Ring 1 - Remaining parts of the operating system
Ring 2 - I/O drivers and utilities
Ring 3 - Applications and programs

Security Modes (used in MAC)

Dedicated security mode:
- All users can access all data.
- Clearance for all information.
- Need to know for ALL data

system high security mode:
- All users can access some data, based on need to know
- Clearance for all information
- Need to know for SOME data

compartmented security mode:
- All users can access some data, based on their need to know and approval.
- Clearance for all information they access
- Need to know for SOME data
- Use of information labels

Multi level:
- All users can access some data, based on their need to know, approval and clearance.
- Clearance for all information they access
- Need to know for SOME data

Others:
controlled type of multilevel security where a limited amount of trust is placed in the system’s hardware/software along with classification
limited access: minimum user clearance is not cleared and the maximum data classification is unclassified but sensitive

Recovery procedures

Recovery procedures: system should restart in secure mode
Startup should occur in maintenance mode that permits access only by privileged users from privileged terminals
Fault-tolerant continues to function despite failure
Fail safe system, program execution is terminated and system protected from compromise when hardware or software failure occurs
Fail soft or resilient system, selected, non-critical processing is terminated when failure occurs
Failover, switches to hot backup.

Assurance
Degree of confidence in satisfaction of security requirements

Evaluation criteria
Trusted Computer System Evaluation Criteria
TCSEC: (Orange book) From the U.S. DoD, it evaluates operating systems, application and systems. It doesn’t touch the network part. It only addresses confidentiality!

- D minimal protection, any systems that fails higher levels
- C1 Discretionary protection (identification, authentication, resource protection).
- C2 – AND Controlled access protection (object reuse, protect audit trail).
- B1 Mandatory protection (security labels) based on Bell-LaPadula security model. Labeled security (process isolation, devices labels).
- B2 AND Structured protection (trusted path, covert channel analysis). Separate operator/admin roles.
- B3 AND security domain (trusted recovery, Monitor event and notification).
- A1 – verified design
- A – verified protection

Operational assurance requirements for TCSEC are:
- System Architecture
- System Integrity
- Covert Channel analysis
- Trusted Facility Management
- Trusted recovery
**Rainbow series:**
Red = trusted network,
Orange = TCSEC evaluation
Brown = trusted facilities management,
Tan = audit,
Aqua = glossary,
Green = password management

**Information Technology Security Evaluation Criteria (ITSEC):**
ITSEC is used in Europe only, not USA. Addresses CIA. Unlike TCSEC it evaluates functionality and assurance separately. Assurance from E0 to E6 (highest) and F1 to F10 (highest). Therefore a system can provide low assurance and high functionality or vice-versa.

**Common Criteria ISO 15408**
Defines a protection profile that specifies the security requirements and protections of a product that is to be evaluated. Organized around TCB entities. Evaluation Assurance Levels (EAL)
- EAL0 - Inadequate assurance
- EAL1 - Functionally tested
- EAL2 - Structurally tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 - Semi formally designed and tested
- EAL6 - Semi formally verified design and tested
- EAL7 - Formally verified design and tested

**Target of Evaluation (TOE):** the product
**Protection Profile (PP):** Security requirements for a class of security devices
**Security Target (ST):** identifies the security properties of TOE
**Security Functional Requirements (SFRs):** Specific individual security functions

### Models

**MATRIX**
Provides access rights to subjects for objects
Access rights are read, write and execute
Columns are ACL’s
Rows are capability lists
Supports discretionary access control

**TAKE-GRANT**
- Uses a direct graph to specify the rights that subjects can transfer to objects or that subjects can take from other subjects
- Uses STATES and STATE TRANSITIONS

**BELL-LAPADULA**
- Confidentiality model
- Developed by DOD, thus classification
- Cannot read up (* property rule AKA CONFINEMENT PROPERTY), exception is a trusted subject.
- Uses access matrix to specify discretionary access control
- Use need to know principle
- Strong star rule: read and write capabilities at the same level
- First mathematical model defined
- Tranquility principle in Bell-Lapadula prevents security level of subjects from being changed once they are created

**BIBA**
- Integrity model
- Cannot read down (simple e=read integrity rule)
- Cannot write up (* integrity)
- Lattice based (least upper bound, greatest lower bound, flow policy)
- Subject at one level of integrity cant invoke subject at a higher level of integrity

**CLARK WILSON**
- Integrity model
- Cannot be tampered, logged, and consistency
- Enforces segregation of duty
- Requires auditing
- Commercial use
- Works with SCI Constrained Data items, data item whose integrity is to be preserved
- Access to objects only through programs

**Information flow model**
Each object is assigned a security class and value, and information is constrained to flow in the directions that are permitted by the security policy. Thus flow off information from one security level to another.

**Covert channels**
Is a way to receive information in an unauthorized manner. Information flood that is not protected by a security mechanism.

2 types
- **Storage covert channel:** processes communicate via storage space on the system
- **Covert timing channel:** one process relays to another by modulating its use of system resources.

**Non interference model**
Groups of users are separated with their commands. Ensures that activities performed at a higher security level do not affect the activities at a lower security level

**Brewer and Nash**
The Chinese Wall model provides a dynamic access control depending on user’s previous actions. This model prevents conflict of interests from members of the same organization to look at information that creates a conflict of another member of that organization. Ex. Lawyers in a law firm with client oppositional

**Other things to know**

Objects of sensitivity labels are: single classification and component set

‘dominate’ in access control means access to higher or equal access class

**Trusted recovery is:** after failure or crash system is still secure

**Security perimeter =** line between TCB and outside

**Validating TCB =** formal for system integrity

**Tempest:** shielding and other emanations-reducing mechanism
Category of Controls

**Preventive** lower the amount and impact of unintended errors and prevent unauthorized intruders to access the systems

**Detective** used to detect an error once it has occurred, operate after the fact. E.g. audit trail

**Corrective** implemented to help mitigate the impact of a loss e.g. restoring data

**Deterrent controls** used to encourage compliance. E.g. using corporate property to store illegal content as porno, entertainment political data

**Administrative Management controls**

**Separation of duties** assigns parts of tasks to different individuals thus no single person has total control of the system’s security mechanisms

**Least privilege** a system’s user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest time. Three types: Read only, Read/write and Access/change

**Two-man control** two persons review and approve the work of each other

**Dual control** two persons are needed to complete a task

**Rotation of duties** limiting the amount of time a person is assigned to perform a security related task before being moved to different task to prevent fraud

**Mandatory vacations** prevent fraud and allowing investigations

**Need to know** the subject is given only the amount of information required to perform an assigned task

**Employment screening or background checks**

**Violation Analysis**

Clipping levels must be established to be effective

Clipping Level – baseline of normal activity, used to ignore normal user errors

**Clipping Based Anomaly Detection**

Looking for:

- Repetitive Mistakes
- Individuals who exceed authority
- Too many people with unrestricted access
- Patterns indication serious intrusion attempts

**Types of system failure**

**System reboot** System shuts itself down in a controlled manner after detecting inconsistent data structures or runs out of resources

**Emergency restart** when a system restarts after a failure happens in an uncontrolled manner. E.g. when a low privileged user tries to access restricted memory segments

**System cold start** when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system in a more consistent state.

**Monitoring and auditing**

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. This baseline is referred to as clipping level

***Audit trails***

- Transaction date/time
- Who processed the transaction
- At which terminal
- Various security events

**Common criteria hierarchical recovery types**

1. **Manual** System administrator intervention is required to return the system to a secure state
2. **Automatic** Recovery to an secure state is automatic when resolving a single failure (though system administrators are needed to resolve additional failures)
3. **Automatic without Undo Loss** Higher level of recovery defining prevention against the undue loss of protected objects

**System recovery after a system crash**

1. Rebooting system in single user mode or recovery console, so no user access is enabled
2. Recovering all file systems that were active during failure
3. Restoring missing or damaged files
4. Recovering the required security characteristic, such as file security labels
5. Checking security-critical files such as system password file

**Trust recovery**

Ensures that the security is not breached when a system crash or failure occurs. Only required for a B3 and A1 level systems

**Failure preparation** Backup critical information thus enabling data recovery

**System shutdown**

Comprises a graceful shutdown (if possible) to ensure data is backed up and only required for a B4 level system

**System recovery**

1. Rebooting system in single user mode or recovery console, so no user access is enabled
2. System shutdown

**Operational Security**

**Other things to know**

OPSEC process: Understanding your day-to-day operations from the viewpoint of a competitor, enemy, or hacker and then developing and applying countermeasures.

Pen-test – testing of network security as would a hacker do to find vulnerabilities. Always get management approval firs!

Port scanner: program that attempts to determine whether any of a range of ports is open on a particular computer or device

Ring zero- inner code of the operating system. Reserved for privileged instructions by the OS itself

War dialer: dials a range of phone numbers as in the movie war-games

Assurance = other word for security

Superzapping: system utility or application that bypasses all access controls and audit/logging functions to make updates to code or data

Operational assurance – Verification that a system is operating according to its security requirements

- Design & development reviews
- Formal modeling
- Security architecture
- ISO 9000 quality techniques
- Assurance – degree of confidence that the implemented security measures work as intended

**Piggybacking**: when an unauthorized person goes through a door behind an authorized person.

**Supervisor mode**: processes running in inner protected ring

**Threats and vulnerabilities**

**Accidental loss** occurs unintentionally

Examples: user input errors deletion errors faulty data or application programs

**Inappropriate activities** computer behavior that does not rise the level of criminal activity, but may ye be grounds for job action or dismissal

- Inappropriate content using corporate property to store illegal content as porno, entertainment political data
- Waste of corporate resources using corporate resources for private use
- Sexual or Racial Harassment using computer resources
- Abuse of Privileges and Rights

**Illegal Computer Operations**

- Eavesdropping – sniffing, dumpster diving, social engineering
- Fraud – collusion, falsified transactions
- Theft – information or trade secrets, physical hardware and software theft
- Sabotage – Denial of Service (DoS), production delays
- External Attacks – malicious cracking, scanning, war dialing

**Types of system failure**

- Too many people with unrestricted access
- Patterns indication serious intrusion attempts

**Administrative Management controls**

**Separation of duties** assigns parts of tasks to different individuals thus no single person has total control of the system’s security mechanisms

**Least privilege** a system’s user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest time. Three types: Read only, Read/write and Access/change

**Two-man control** two persons review and approve the work of each other

**Dual control** two persons are needed to complete a task

**Rotation of duties** limiting the amount of time a person is assigned to perform a security related task before being moved to different task to prevent fraud

**Mandatory vacations** prevent fraud and allowing investigations

**Need to know** the subject is given only the amount of information required to perform an assigned task

**Employment screening or background checks**

**Violation Analysis**

Clipping levels must be established to be effective

Clipping Level – baseline of normal activity, used to ignore normal user errors

**Clipping Based Anomaly Detection**

Looking for:

- Repetitive Mistakes
- Individuals who exceed authority
- Too many people with unrestricted access
- Patterns indication serious intrusion attempts

**Types of system failure**

- System reboot: System shuts itself down in a controlled manner after detecting inconsistent data structures or runs out of resources
- Emergency restart: when a system restarts after a failure happens in an uncontrolled manner. E.g. when a low privileged user tries to access restricted memory segments
- System cold start: when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system in a more consistent state.

**Monitoring and auditing**

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. This baseline is referred to as clipping level

***Audit trails***

- Transaction date/time
- Who processed the transaction
- At which terminal
- Various security events

**Common criteria hierarchical recovery types**

1. Manual: System administrator intervention is required to return the system to a secure state
2. Automatic: Recovery to an secure state is automatic when resolving a single failure (though system administrators are needed to resolve additional failures)
3. Automatic without Undo Loss: Higher level of recovery defining prevention against the undue loss of protected objects

**System recovery after a system crash**

1. Rebooting system in single user mode or recovery console, so no user access is enabled
2. Recovering all file systems that were active during failure
3. Restoring missing or damaged files
4. Recovering the required security characteristic, such as file security labels
5. Checking security-critical files such as system password file

**Trust recovery**

Ensures that the security is not breached when a system crash or failure occurs. Only required for a B3 and A1 level systems

**Failure preparation** Backup critical information thus enabling data recovery

**System shutdown**

Comprises a graceful shutdown (if possible) to ensure data is backed up and only required for a B4 level system

**System recovery**

1. Rebooting system in single user mode or recovery console, so no user access is enabled
2. System shutdown

**Operational Security**

**Other things to know**

OPSEC process: Understanding your day-to-day operations from the viewpoint of a competitor, enemy, or hacker and then developing and applying countermeasures.

Pen-test – testing of network security as would a hacker do to find vulnerabilities. Always get management approval firs!

Port scanner: program that attempts to determine whether any of a range of ports is open on a particular computer or device

Ring zero- inner code of the operating system. Reserved for privileged instructions by the OS itself

War dialer: dials a range of phone numbers as in the movie war-games

Assurance = other word for security

Superzapping: system utility or application that bypasses all access controls and audit/logging functions to make updates to code or data

Operational assurance – Verification that a system is operating according to its security requirements

- Design & development reviews
- Formal modeling
- Security architecture
- ISO 9000 quality techniques
- Assurance – degree of confidence that the implemented security measures work as intended

**Piggybacking**: when an unauthorized person goes through a door behind an authorized person.

**Supervisor mode**: processes running in inner protected ring
Configuration Change Management – Required B2, B3 and A1
- Process of tracking and approving changes
- Identify, control and audit changes
- Changes to the system must not diminish security
- Includes roll back procedures
- Documentation updates to reflect changes
- Recommended for systems below the required B2, B3 and A1
- Change Control Functions:
  - Orderly manner and formalized testing
  - Users informed of changes
  - Analyze effects of changes
  - Reduce negative impact of changes
- Configuration Management required for Development and Implementation stages for B2 and B3
- Configuration Management required for life cycle of system for A1

Resource Protection
Protecting Resources from disclosure alteration or misuse
- Hardware – routers, firewalls, computers, printers
- Software – libraries, vendor software, OS software
- Data Resource – backup data, user data, logs

Hardware Controls
Hardware Maintenance
- Requires physical and logical access by support and vendors / Supervision of vendors and maintenance, background checks
- Maintenance Accounts
- Disable maintenance accounts when not needed
- Rename default passwords
Diagnostic Port Control
- Specific ports for maintenance
- Should be blocked from external access

Hardware Physical Controls – require locks and alarms
- Sensitive operator terminals
- Media storage rooms
- Server and communications equipment
- Modern pools and circuit rooms

Software Controls
Anti-virus Management – prevent download of viruses
Software Testing – formal rigid software testing process
Software Utilities – control of powerful utilities
Safe software Storage – prevent modification of software and copies of backups
Back up Controls – test and restore backups

Privileged Entity Controls – “privileged operations functions”
- Extended special access to system commands
- Access to special parameters
- Access to system control program – some only run in particular state

Media Resource Protection
Media Security Controls – prevent the loss of sensitive information when the media is stored outside the system
- Logging – log the use of the media; provides accountability
- Access Control – physical access control
- Proper Disposal – sanitization of data – rewriting, degaussing, destruction

Media Viability Controls – protect during handling, shipping and storage
- Marking – label and mark media, bar codes
- Handling – physical protection of data
- Storage – security and environmental protection from heat, humidity, liquids, dust, smoke, magnetism

Physical Protection
Protection from physical access
- Hardware – routers, firewalls, computers, printers
- Software – libraries, vendor software, OS software
- Physical piggybacking – following an authorized person through a door

Penetration Testing
Testing a networks defenses by using the same techniques as external intruders
- Scanning and Probing – port scanners
- Demon Dialing – war dialing for modems
- Sniffing – capture data packets
- Dumpster Diving – searching paper disposal areas
- Social Engineering – most common, get information by asking

Problem Management
Goals of problem management:
- Reduce failures to a manageable level
- Prevent occurrence of a problem
- Mitigate the impact of problems

Potential Problems:
- Performance and availability of computing resources
- The system and networking infrastructure
- Procedures and transactions
- Safety and security of personnel

Abnormal Events - that can be discovered by an audit
- Degraded resource availability
- Deviations from the standard transaction procedures
- Unexplained occurrences in a processing chain

Objective of problem management is resolution of the problem
**Software Life Cycle Development**

**MODELS**
- Simplistic model
  - This model was simplistic in that it assumed that each step could be completed and finalized without any effect from the later stages that may require rework.
- Waterfall model
  - Can be managed if developers are limited going back only one step. If rework may be done at any stage it’s not manageable. Problem: it assumes that a phase or stage ends at a specific time.
- System Requirements -> Software Requirements -> Analysis -> Program Design -> Coding -> Testing -> Operations & Maintenance
- Waterfall including Validation and Verification (V&V)
  - Reinterpretation of the waterfall model where verification evaluates the product during development against specification and validation refers to the work product satisfying the real-world requirements and concepts.
- Spiral model
  - Angular = progress made
  - Radial = cost
  - Lower left = development plans
  - Upper left = objectives of the plans, alternatives checked
  - Upper right = assessing alternatives, risk analysis
  - Lower right = final development
  - Left horizontal axis = includes the major review required to complete each full cycle

**LIFECYCLE**
- Information security in Lifecycle Management
  - Conception phase: Policies, standards, threats vulnerabilities
  - Development phase: incorporate security specs. Determine access controls, verification
  - Implementation phase: install security software
  - Testing phase: test security software and controls, documentation
  - Maintenance phase: revalidate controls pen test, change process
- Testing issues
  - Personnel separate from developers should test.
  - Should also check for incorrect data types and data out of range (live of actual data might not do so)
- UNIT TESTING: testing small piece of software during a development stage by developers and quality assurance
- Maintenance and change control
  - Request control: manages users requests, sets priority, costs and interface

**Object-Orientated systems**
- Objects behave as black box; they are encapsulated to perform an action. Can be substituted if they have compatible operations. It can store objects like video and pictures
- Message: communication to object to perform an action
- Method: code that defines an action an object performs in response to a message
- Behavior: results exhibited by an object in response to a message
- Class: collection of methods that defines the behavior of objects
- Instance: objects are instances of classes that contain their methods
- Inheritance: methods from a class are by subclass
- Multiple Inheritance: class inherits characteristics from more than one parent class
- Delegation: forwarding a request to another object
- Polymorphism: objects of many different classes are related by some common super class.

**Security Life Cycle Components**
- System feasibility: ISP, Standards, Legal, validation concepts
- Software Plans & Requirements: Due diligence, Threats, Security requirements
- Product Design: incorporate security specs, Design docs, Determine access controls, Verification
- Detailed Design: Design access controls & security controls, detailed docs, verification, Consider BCP, employ encryption
- Coding: Unit testing, Support BCP, develop docs
- Integration product: Refine docs, integrate security, security verification, test integrated modules
- Implementation: Install, Test security, Run system, Acceptance testing, Complete documentation, certification, and accreditation
- Operations & Maintenance: Pen test, Change control, update docs, recertification, revalidate security controls

**Change control**
- recreating and analyzing the problem, developing the change, quality control, tools, documentation, restrictions andrecertification and accreditation if necessary

**Release control**
- issuing latest release of software

**Configuration management**
- Configuration item (CI) component whose state is recorded
- Version: recorded state of the CI
- Configuration: collection of component CI’s that make another CI
- Building: assembling a version of a CI using component CI’s
- Build list: set of versions of component CI’s used to build a CI
- Software Library: controlled area only accessible for approved users

**Software capability maturity model (CMM)**
- Quality of software is a direct function of quality of development
- Defined by Carnegie Mellon University SEI (Software Engineering Institute)
- Describes procedures, principles, and practices that underlie software development process maturity

**5 levels**
1. initiating – competent people, informal processes ad-hoc
2. repeatable – project management processes
3. defined – engineering processes
4. managed – product and process improvement, quantitatively controlled
5. Optimizing – continuous process improvement

**Conclusion**
- Object orientation (e.g. with C++ and Smalltalk) supports reuse of objects and reduces development risk, natural in its representation of real world entities.
- Cohesion: ability to perform without use of other programs
  - High cohesion: without use of other modules
  - Low cohesion: Must interact with other modules

**Coupling:**
- affect on other modules.
  - High coupling: module largely affects many more modules
  - Low coupling: it doesn’t affect many other

**Poly-instantiation**:
- development of detailed version of an object from another object using different values in the new object

**5 phases of object orientation**
- Requirements analysis (OORA) defines classes of objects and their interactions
- Analysis (OOA) understanding and modeling a particular problem
- Domain Analysis (DA) seeks to identify classes and objects that are common to all applications in a domain
- Design (OOD) objects are the basic units, and instances of classes
- Programming (OOP) employment of objects and methods

If class = airplane, objects like fighter plane, cargo plane, passenger plane can be created. Method would be what a plane would do with a message like: climb, dive, and roll.

**Object Request Brokers (ORBs):** middleware that acts as locators and distributors of the objects across networks.

**Common object request broker (CORBA) architecture enables**
- programs written in different languages and using different platforms and OS’s through IDL (Interface Definition Language)
- Common object Model (COM) support exchange of objects amongst programs. This used to be called OLE. DCOM is the network variant (distributed)

**Conclusion:** Object orientation (e.g. with C++ and Smalltalk) supports reuse of objects and reduces development risk, natural in its representation of real world entities.
**Artificial intelligence systems**

**Expert Systems**
- Based on human reasoning
- Knowledge base of the domain in the form of rules
- If-then statements called forward chaining
- Priority in rules are called salience
- Interference system = decision program
- Expert system = inference engine + knowledge base
- Degree of uncertainty handled by approaches as Bayesian networks (probability of events), certainty factors (probability an event is true) or fuzzy logic (to develop conclusions)
- Two modes:
  - Forward chaining: acquires info and comes to a conclusion
  - Backward chaining: backtracks to determine if a hypothesis is correct

**Neural Networks**
- Based on function of biologic neurons
- Works with weighted inputs
- If a threshold is exceeded there will be output
- Single-layer: only one level of summing codes
- Multi-level: more levels of summing codes
- Training period needed to determine input vectors
- Adaptability (learning process)

**Database systems**

**DBMS**: refers to a suite of software programs that maintains and provides controlled access to data components store in rows and columns of a table

**Types**
- Hierarchical: tree (sons with only one parent)
- Network = tree (all interconnected)
- Mesh
- Object-oriented
- Relational – has DDL and DML, has TUPLES and ATTRIBUTES (rows and columns)

**DDL – Data definition language** defines structure and schema
**DML – Data manipulation language** view, manipulate and use the database via VIEW, ADD, MODIFY, SORT and DELETE commands.
**DDE – Dynamic data exchange** enables applications to work in a client/server model by providing the interprocess communications mechanism (IPC)
**DCL – Data control language** subset of SQL used to control access to data in a database, using GRANT and REVOKE statements

**Database Security Issues**

Security can be provided through Views. That is a virtual relation that combines information from other relations. A view can be used to restrict data made available for users based on their privileges and need-to-know.

- Operations: join, project and select (JPS)
- Views will hide information that a user is not allowed to see, thus implementing the LEAST Privilege.
- Granularity: the fineness with in which access can be controlled or limited
- Aggregation: is the act of obtaining information of a higher sensitivity by combining information of lower levels of sensitivity.
- Inference: use the ability of users to deduce information about data at unauthorized levels using inference channels

**Data warehousing**

Database warehousing is a repository of information from heterogeneous databases that is available for users for making queries. 

- Data is normalized (Ensures that attributes in a table only depend on the primary key)

**Data mining**

Data mining is searching for data correlations in the data warehousing.

- The correlation of data about data is called metadata.
- Can be stored in a separate database with high levels of protection called the Data mart. 
- The information obtained from data marts can be send back to the data warehouse

**Data dictionaries**

Data dictionary is a database for system developers. It records all data structures used by an application. If a data dictionary is separated, the primary dictionary provides the baseline of the data and the central control, the secondary dictionary to separate development projects, provide backup for primary and to serve as a partition between the development and test databases

**Centralized Architecture**

Centralized systems are less difficult to protect because they are not interconnected through a network

Distributed systems are interconnected through a network.

**Database Security Issues**

Security can be provided through Views. That is a virtual relation that combines information from other relations. A view can be used to restrict data made available for users based on their privileges and need-to-know.

- Operations: join, project and select (JPS)
- Views will hide information that a user is not allowed to see, thus implementing the LEAST Privilege.
- Granularity: the fineness with in which access can be controlled or limited
- Aggregation: is the act of obtaining information of a higher sensitivity by combining information of lower levels of sensitivity.
- Inference: use the ability of users to deduce information about data at unauthorized levels using inference channels

**Data warehousing**

Database warehousing is a repository of information from heterogeneous databases that is available for users for making queries. 

- Data is normalized (Ensures that attributes in a table only depend on the primary key)

**Data mining**

Data mining is searching for data correlations in the data warehousing.

- The correlation of data about data is called metadata.
- Can be stored in a separate database with high levels of protection called the Data mart. 
- The information obtained from data marts can be send back to the data warehouse

**Data dictionaries**

Data dictionary is a database for system developers. It records all data structures used by an application. If a data dictionary is separated, the primary dictionary provides the baseline of the data and the central control, the secondary dictionary to separate development projects, provide backup for primary and to serve as a partition between the development and test databases

**Centralized Architecture**

Centralized systems are less difficult to protect because they are not interconnected through a network

Distributed systems are interconnected through a network.

**Real-time systems**

Acquire data from transducers or sensors in real time, and then making computations and control decisions in a fixed time window. (e.g. fly-by-wire on airplanes)

- Availability is crucial; hence RAID systems are in place.
- Fault tolerant: the system has to detect a fault and take action to recover
- OLTP Online Transaction Processing: clustered databases to provide fault tolerance and high performance. Insure that transactions happen properly or not at all.
- Transactions sometimes described as ideally ACID
  - Atomic: divides transactions into units of work, all modifications take effect or none ( then a rollback)
  - Consistent: all records follow integrity constraints
  - Isolated: transactions executed in isolation until completed
  - Durable: not reversible once committed

**Things to know**

Noise and perturbation: inserting bogus information to hope to mislead an attacker

FIRST step by change process = management approval

- PROTOTYPING: customer view taken into account
- SQL - SUDIGR
  - Select, Update, Delete, Insert, Grant, Revoke
  - Bind variables are placeholders for literal values in SQL query being sent to the database on a server

- Bind variables in SQL used to enhance performance of a database
  - Monitor progress and planning of projects through GANTT and PERT charts
  - Check digit: point of verification in an computerized application
  - Semantic integrity: make sure that the structural and semantic rules are enforced on all data types, logical values that could adversely affect the structure of the database

- Referential integrity: all foreign keys reference existing primary keys
  - Foreign and primary keys uniquely identify a record in a database

- Dynamic Lifetime Objects: Objects created on the fly by software in an Object Oriented Programming environment. An object is preassembled code that is a self-contained module
Mobile code
Java – sandboxes, no warnings, programs are compiled to byte-code
ActiveX – Authenticode, relies on digital signatures, annoying dialogs people click away

Malicious code threats
Virus reproduces using a host application. It inserts or attaches itself to the file
Worm reproduces on its own without host application
Logic Bomb/Code Bomb executes when a certain event happens (like accessing a bank account) or a data/time occurs
Trojan Horse program disguised as a useful program/tool

HOAXES – False warnings like: DON’T OPEN X SEND TO ALL YOUR COLLEAGUES
Remote Access Trojan (RAT) remote control programs that have the malicious code and allow for unauthorized remote access Back orifice, sub seven, net bus
Botnet compromise thousands of systems with zombie codes can be used in DDOS attacks or spammers

Buffer Overflow Excessive information provided to a memory buffer without appropriate bounds checking which can result in an elevation of privilege. If executable code is loaded into the overflow, it will be run as if it were the program.
Buffer overflows can be detected by disassembling programs and looking at their operations.
Buffer overflows must be corrected by the programmer or by directly patching system memory.

Trap Door An undocumented access path through a system. This typically bypasses the normal security mechanisms and is to plant any of the malicious code forms.

Backdoor program installed by an attacker to enable him to come back on a later date without going through the proper authorization channels

Covert Channel Is a way to receive information in an unauthorized manner. Information flood that is not protected by a security mechanism.
Covert Storage Channel Writing to storage by one process and reading by another of lower security level.
Covert Timing Channel One process relays to another by modulating its use of system resources.
Countermeasures: EAL0 systems have less than EAL3 systems because covert channels are normally a flaw in design.
LOKI is a tool used for covert channel that writes data directly after the ICMP header

Virus
Boot sector – moves or overwrites the boot sector with the virus code.
System infector – infects BIOS command other system files. It is often a memory resident virus.
Compression – appended to executables
Companion virus - A specific type of virus where the infected code is stored not in the host program, but in a separate ‘companion’ files. For example, the virus might rename the standard NOTEPAD.EXE file to NOTEPAD.EXD and create a new NOTEPAD.EXE containing the virus code. When the user subsequently runs the Notepad application, the virus will run first and then pass control to the original program, so the user doesn’t see anything suspicious. Takes advantage of search order of an OS
Stealth virus – hides modifications to files or boot records and itself
Multipart virus - infects both the boot sector and executable files; becomes resident first in memory and then infects the boot sector and finally the entire system
Self-garbling virus – attempts to hide by garbling its code; as it spreads, it changes the way its code is encoded
Polymorphic virus – this is also a self-garbling virus where the virus changes the “garble” pattern each time it spreads. As a result, it is also difficult to detect.
Macro virus – usually written in Word Basic, Visual Basic or VBScript and used with MS Office
Resident virus – Virus that loads when a program loads in memory
Non-resident virus - attached to .exe

ANTI-Virus
Signature based cannot detect new malware
Heuristic behavioral can detect new malware

System Development Life Cycle
Project initiation: Feasibility, cost, risk analysis, Management approval, basic security objectives
Functional analysis and planning: Define need, requirements, review proposed security controls
System design specifications: Transform detailed design specs, Review support documentation, Examine security controls
Software development: Programmers develop code. Unit testing Check modules. Prototyping, Verification, Validation
Acceptance testing and implementation: Separation of duties, security testing, data validation, bounds checking, certification, accreditation
Operations and maintenance: release into production. Certification/accreditation
Revisions/ Disposal: remove. Sanitation and destruction of unneeded data

Software Life Cycle
Requirements
Design
Programming
Testing
Conversion
Operations
Maintenance

More things to know
- Black-box testing observes the system external behavior.
- White-box testing is a detailed exam of a logical path, checking the possible conditions.
- Compiled code poses more risk than interpreted code because malicious code can be embedded in the compiled code and can be difficult to detect.
- Regression testing is the verification that what is being installed does not affect any portion of the application system already installed. It generally requires the support of automated process to repeat tests previously undertaken.
- Code comparison is normally used to identify the parts of the source code that have changed.
- Integration testing is aimed at finding bugs in the relationship and interfaces between pairs of components. It does not normally test all functions.
- Unit testing is the testing of a piece of code. It will only detect errors in the piece of code being tested.

<table>
<thead>
<tr>
<th>Control</th>
<th>Accuracy</th>
<th>Security</th>
<th>Consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventative</td>
<td>Data checks, validity checks</td>
<td>Labels, traffic padding, encryption</td>
<td>DBMS, data dictionary</td>
</tr>
<tr>
<td>Detective</td>
<td>Cyclic Redundancy</td>
<td>IDS, audit trails</td>
<td>Comparison tools</td>
</tr>
<tr>
<td>Corrective</td>
<td>Checkpoint, backups</td>
<td>Emergency response</td>
<td>Database controls</td>
</tr>
</tbody>
</table>
**DRIVERS**

- Business need to minimize loss.
  - Online service providers like Google and eBay and NYSE need to be online
  - Retain value. Customer records = high value, lost data reduces brand quality
- Regulatory compliance
  - Utility companies (gas energy water)
  - Government (FISMA, NIST)
  - Finance (sox, FFIEC Basel II)
  - Healthcare (HIPAA)

**BCP**

Plan for emergency response, backup operations and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

**NIST**

3 Phases of actions
- Notification/activation
- Recovery
- Reconstitution (back up and running)

**BCP&DRP Goals**

Business continuity- Ensuring the business can continue in an emergency
- Focus on business processes
- Scope/plan initiation
- Part of your security program
- Need for management support
- BIA – business impact analysis
- BCP Development
- At least once a year testing

**Roles and responsibilities**

**BCP committee**
- Senior staff (ultimate responsibility, due care/diligence)
- Various business units (identify and prioritize time critical systems)
- Information Systems
- Security Administrator
- People who will carry out the plan (execute)
- Representatives from all departments

**Role of IT department**

- Make sure that adequate backup restore processes are available, including off-site media storage
- Employ sufficient physical security mechanisms to protect network and hardware components
- Ensure that the organization uses sufficient logical security measures for protecting sensitive data
- Ensure that departments implements adequate system administration, including up-to-date inventories of hardware, software and media storage

**BCP goals**

- Prevent interruption to normal business activity and critical business process
- Minimize the effects of a disaster
- Quick recovery of all business
- Should cover:
  - #1 PEOPLE (ALWAYS FIRST)
  - LAN/Wan
  - Telecom, data links
  - Workstations and workspace
  - Application software and DATA
  - Media and record storage
  - Staff duties

**BCP elements**

1. **Scope and plan initiation** - Consider amount of work required, resources required, management practice
2. **BIA** – helps to understand impact of disruptive processes
   - Use BIA to develop BCP
   - Testing
3. **Business Continuity Plan development**
   - Use BIA to develop BCP
   - Testing
4. **Plan approval and implementation**
   - Management approval
   - Create awareness
   - Update plan as needed

**Threats**

Natural (Fires, explosions water, storm)
Man made (bombing, strikes, toxin spills)

**BIAS**

Goal: to create a document to be used to help understand what impact a disruptive event would have on the business
- Gathering assessment material
  - Org charts to determine functional relationships
  - Examine business success factors
- Vulnerability assessment
  - Identify Critical IT resources out of critical processes
  - Identify disruption impacts and Maximum Tolerable Downtime (MTD)
  - Loss Quantitative (revenue, expenses for repair) or qualitative (competitive edge, public embarrassment). Presented as low, high, medium.
- Develop recovery procedures
- Analyze the compiled information
  - Document the process
  - Identify inter-dependability
  - Determine acceptable interruption periods
- Documentation and Recommendation
  - Presentation to management

**Business Continuity plans development**

- Defining the continuity strategy
  - Computing: strategy to preserve the elements of hardware/software/communication lines/applications/data
  - Facilities: use of main buildings or any remote facilities
  - People: operators, management, technical support persons
  - Supplies and equipment: paper, forms HVAC
- Documenting the continuity strategy
Disaster Recovery Planning
Statement of actions that have to be taken before, during and after a disruptive event that causes a significant loss of information. Goal: provide organized way for decision making, reduce confusion and deal with the crisis. Planning and development must occur before the disaster.
BIA has already been done, now were going to protect!

Disaster Planning Process
- Disaster Processing Continuity plan
- Disaster Recovery plan maintenance

Disaster Processing Continuity plan
Mutual aid agreements (aka reciprocal agreement)
Arrangement with another similar corporation to take over processes. Advantage: cheap. Disadvantage: must be exact the same, is there enough capability, only for short term and what if disaster affects both corporations. Is not enforceable.

Subscription services
Third party, commercial services provide alternate backups and processing facilities. Most common of implementations!
- HOT SITE: Fully configured computer facility. All applications are installed, up-to-date mirror of the production system. For extremely urgent critical transaction processing. Advantage: 24/7 availability and exclusive use are assured. Short and long term.
Disadvantage: extra administrative overhead, costly. Security controls need to be installed at the remote facility too. Exclusive to one company.
- WARM SITE: Cross between hot and cold site. The computer facility is available but the applications may not be installed or need to be configured. External connections and other data elements that take long time to order are present. Workstations have to be delivered and data has to be restored. Advantage: Less costly, more choices of location, less administrative resources.
Disadvantage: it will take some time to start production processing. Nonexclusive.
- COLD SITE: Least ready but mostly used. Has no hardware installed only power and HVAC. Disadvantage: Very lengthy time of restoration, false sense of security but better than nothing. Advantage: Cost, ease of location choice. Nonexclusive

Multiple centers (aka dual sites)
Processing is spread over several computer centers. Can be managed by same corporation (in-house) or with another organization (reciprocal agreement). Advantage: costs, multiple sites will share resources and support. Disadvantage: a major disaster could affect both sites; multiple configurations have to be administered.

Service bureaus
Contract with a service bureau to fully provide alternate backup processing services. Advantage: quick response and availability. Testing is possible. Disadvantage: expense and it is more of a short time option.

Other data center backup alternatives
- Rolling/mobile sites. Mobile homes or HVAC trucks. Could be considered a cold site.
- In-house or external supply of hardware replacements. Stock of hardware either onsite or with a vendor. May be acceptable for warm site but not for hot site.
- Prefabricated buildings. A very cold site.

Transaction Redundancy Implementations
Electronic vaulting transfer of backup data to an offsite storage location via communication lines.
Remote Journaling parallel processing of transactions to an alternative site via communication lines.
Database shadowing live processing of remote journaling and creating duplicates the database sets to multiple servers.

Disaster recovery plan test types
1. Checklist test copies of the plan are distributed to management for review.
2. Structured Walk-Through test business unit management meets to review the plan.
3. Simulation test all support personnel meet in a practice room.
4. Parallel test Critical systems are run at an alternate site
5. Full- Interruption test Normal production shut down, with real disaster recovery processes.

Disaster recovery plan test types
1. Checklist test copies of the plan are distributed to management for review.
2. Structured Walk-Through test business unit management meets to review the plan.
3. Simulation test all support personnel meet in a practice room.
4. Parallel test Critical systems are run at an alternate site
5. Full- Interruption test Normal production shut down, with real disaster recovery processes.

Backup types
Full All files, archive bit and modify bit are cleared. Advantage: only previous day needed for full restore, disadvantage: time consuming.
Incremental only modified files, archive bit cleared, Advantage: least time and space, Disadvantage: first restore full then all incremental backups, thus less reliable because it depends on more components.
Differential: only modified files, doesn't clear archive bit. Advantage: full and only last diff needed, Intermediate time between full and diff.

Disaster recovery process
TEAMS
Recovery team mandated to implement recovery after the declaration of the disaster.
Salvage team goes back to the primary site to normal processing environmental conditions. Clean, repair, Salvage. Can declare when primary site is available again.

Normal Operations Resume plan has all procedures on how the company will return processing from the alternate site.

Other recovery issues
Interfacing with other groups: everyone outside the corporation.
Employee relations: responsibility towards employees and their families.
Fraud and Crime: like vandalism, looting and people grabbing the opportunity.
Financial disbursement.
Media relations.

Things to know
The disaster is not over until all operations have been returned to their normal location and function.
It will be officially over when the data has been verified at the primary site as accurate.

RTO: recovery time objectives. Refers to business processes not hardware.
RTO 5 minutes or hours ➔ Hot site; RTO 1-2 days ➔ warm site.
RTO 3-5 days ➔ mobile site; RTO 1-2 weeks ➔ cold site.

Backup storage media
Tape: sequential, slow read, fast write 200GB an hour, historically cheaper than disk (now changing), robotic libraries.
Disk: fast read/write, less robust than tape.
Optical drive: CD/DVD. Inexpensive.
Solid state: USB drive, security issues.

MTT (mean time to failure)
MTTR (mean time to repair)
MTBF (mean time before failures) = MTTF + MTTR
RPO - Recovery Point Objective: Point in time that application data must be recovered to resume business functions.
MTD - Maximum Tolerable Downtime: Maximum delay a business can be down and still remain viable.
MTD minutes to hours: critical.
MTD 24 hours: urgent.
MTD 72 hours: important.
MTD 7 days: normal.
MTD 30 days: non-essential.
### Terms
- **Wire Tapping** eavesdropping on communication—only legal with prior consent or warrant
- **Dumpster Driving** act of going through someone's trash to find useful or confidential info—it is legal but unethical in nature
- **Phishing** act of sending spoofed messages that pretend to originate from a source the user trusts (like a bank)
- **Social Engineering** act of tricking someone into giving sensitive or confidential info that may be used against the company
- **Script kiddie** someone with moderate hacking skills, gets code from the Internet.
- **Data Diddling** act of modifying information, programs, or documents to commit fraud, tampers with INPUT data
- **Privacy Laws** data collected must be collected fairly and lawfully and used only for the purpose it was collected.
- **Computer Crime Laws** -3 types of harm
  - unauthorized intrusion,
  - unauthorized alteration or destruction
  - malicious code
- **Admissible evidence** relevant, sufficient, reliable
- **Red boxing:** pay phones cracking
- **Black Boxing** manipulates toll-free line voltage to phone for free
- **Blue Boxing** tone simulation that mimics telephone co. system and allows long distance call authorization
- **Phreakers** hackers who commit crimes against phone companies
- **Salami removal** of a small amount of money otherwise known as skimming
- **Hearsay** second-hand data not admissible in court
- **Federal Sentencing** provides judges and courts procedures on
- **Guidelines** the prevention, detection and reporting of crimes that should occur by a company official and made company executives responsible for the company's actions
- **Due Care** Which means when a company did all that it could have reasonably done to try and prevent security breach / compromise / disaster, let's call it damage and took the necessary steps required as countermeasures / controls, let's call it safeguards. The benefit of "due care" can be seen as the difference between the damage with or without out "due care" safeguards in place. AKA doing something about the threats
- **Due Diligence** means that the company properly investigated all of its possibly weaknesses and vulnerabilities AKA understanding the threats
- **Enticement** the legal action of luring an intruder, like in a honey pot
- **Entrapment** the illegal act of inducing a crime, the individual had no intent of committing the crime at first

### Ethics
- **Code of Ethics Canons:**
  - Protect society, the commonwealth, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.

- **Internet Advisory Board (IAB):**
  - Access to and use of Internet is a privilege and should be treated as such.
  - It is defined as unacceptable and unethical if you for example gain unauthorized access to resources on the internet, destroy integrity waste resources or compromise privacy.

- **Corporate Officer Liability**
  - Executives are now held liable if the organization they represent is not compliant with the law.
  - Negligence occurs if there is a failure to implement recommended precautions, if there is no contingency/disaster recovery plan, failure to conduct appropriate background checks, failure to institute appropriate information security measures, failure to follow policy or local laws and regulations.

### Intellectual property laws
- **Patent** grants ownership of an invention and provides enforcement for owner to exclude others from practicing the invention. After 20 years the idea is open source
- **Copyright** protects the expression of ideas but not necessarily the idea itself
- **Trademark** something that is propriety to a company and important for its survival and profitability (like formula of Coke or Pepsi)

### Incident Response
- **Events:** anything that happens. Can be documented verified and analyzed
- **Incident:** event or series of events that adversely impact the ability of an organization to do business
- **Framework:**
  - **Response Capability** (policy, procedures, a team),
  - **Incident response and handling** (Triage, investigation, containment, and analysis & tracking),
  - **Recovery** (Recovery / Repair),
  - **Debriefing / Feedback** (External Communications, Metrics)

### Regulations
- **SOX 2002 after ENRON and World Online debacle** Independent review by external accountants.
  - Section 302: CEO’s CFO’s can be sent to jail when information they sign is incorrect.
  - Section 404 is the about internal controls assessment: describing logical controls over accounting files; good auditing and information security.
  - Need for information security to protect the individual.

### Law
- **Common law:** USA, UK Australia Canada (judges)
- **Civil law:** Europe, south America
- **Islamic and other Religious laws:** middle east Africa Indonesia
- **USA**
  - 3 branches for laws:
    - Legislative: writing laws (statutory laws).
    - Executive: enforces laws (administrative laws)
    - Juridical: Interprets laws (makes common laws out of court decisions)
  - 3 categories
    - **Criminal law**—individuals that violate government laws.
    - **Civil law**—wrongs against individual or organization that result in a damage or loss. Punishment can include financial penalties. AKA tort law (I’ll Sue You!) Jury decides upon liability
    - Administrative/Regulatory law—how the industries, organizations and officers have to act. Wrongs can be penalized with imprisonment or financial penalties
<table>
<thead>
<tr>
<th>Evidence</th>
<th>Investigation</th>
<th>FAIR Information Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient –persuasive enough to convince one of the validity of the findings</td>
<td>MOM means, opportunity and motive</td>
<td>• Openness</td>
</tr>
<tr>
<td>Reliable –consistent with fact</td>
<td>Determine suspects</td>
<td>• Collection Limitation</td>
</tr>
<tr>
<td>Relevant –relationship to the findings must be reasonable and sensible</td>
<td>Victimology –why certain people are victims of crime and how lifestyle affects the chances that a certain person will fall victim to a crime investigation</td>
<td>• Purpose Specification</td>
</tr>
<tr>
<td>Permissible – lawful obtaining of evidence</td>
<td>Target Risk Assessment –why was target chosen –history of target</td>
<td>• Use Limitation</td>
</tr>
<tr>
<td>Preserved and identifiable – collection, reconstruction</td>
<td>Relevant</td>
<td>• Data Quality</td>
</tr>
</tbody>
</table>

**Evidence Lifecycle**

1. Discovery
2. Protection
3. Recording
4. Collection and identification
5. Analysis
6. Storage, preservation, transportation
7. Present in court
8. Return to owner

**Types of evidence**

**Best Evidence:**
- Primary Evidence–is used at the trial because it is the most reliable.
- Original documents–are used to document things such as contracts–NOTE: no copies!
- Note: Oral is not best evidence though it may provide interpretation of documents, etc.

**Secondary Evidence**
- Not as strong as best evidence.
- A copy, Secondary Evidence, is not permitted if the original, Best Evidence, is available
- Copies of documents.
- Oral evidence like Witness testimony

**Direct Evidence:**
- Can prove fact by itself and does not need any type of backup information.
- Testimony from a witness—one of their 5 senses:
  - Oral Evidence is a type of Secondary Evidence so the case can’t simply stand on it alone.
  - But is it Direct Evidence and does not need other evidence to substantiate it

**Conclusive evidence**
- Irrefutable and cannot be contradicted
- Requires no other corroboration

**Circumstantial evidence**
- Used to help assume another fact
- Cannot stand on its own to directly prove a fact

**Corroborative Evidence:**
- Supports or substantiates other evidence presented in a case

**Hearsay Evidence**
- something a witness hear another one say.
- Also business records are hearsay and all that’s printed or displayed.
- One exception to business records: audit trails and business records are not considered hearsay when the documents are created in the normal course of business.

**Witnesses**

**Opinion Rule**
- Requires witnesses to testify only about the facts of the case, cannot be used as evidence in the case.

**Expert Witnesses**
- Used to educate the jury, can be used as evidence.

**Admissibility of evidence**
- For evidence to be admissible it must be:
  - Relevant
  - Proof of crime, documentation of events, proof of acts and methods used, motive proof, identification of acts
  - Legally permissible obtained in a lawful manner
  - Avoid: unlawful search and seizure, secret recording, privacy violations, forced confessions, unlawful obtaining of evidence
  - Reliable evidence has not been tampered with or modified

**Identification**
- labeling, recording serial number etc.

**Evidence must be preserved and identifiable**
- Collection, documentation, classification, comparison, reconstruction
- Witnesses that evidence is trustworthy, description of procedures, normal business methods collections, error precaution and correction

**Laws**
- 1974 US Privacy Act: Protection of PII on federal databases
- 1980 Organization for Economic Cooperation and Development (OECD): Provides for data collection, specifications, safeguards
- 1986 (amended in 1996) US Computer Fraud and Abuse Act: Trafficking in computer passwords or information that causes a loss of $1,000 or more or could impair medical treatment.
- 1986 Electronic Communications Privacy Act: Prohibits eavesdropping or interception w/o distinguishing private/public
- 1996 US Economic and Protection of Proprietary Information Act: Air and corporate espionage
- US Government has power to regulate all trade between states.

**Investigating**

**Interviewing**
- To ultimately obtain a confession, discover information

**Interrogation**
- Evidence retrieval method

**The Process**
- Prepare questions and topics, put witness at ease, summarize information
- Have one person as lead and 1-2 others involved as well
- Never interrogate or interview alone

**Things to know**

**Hackers and crackers**
- Want to verify their skills as intruders

**Notebook**
- most preferred in the legal investigation is a bound notebook, pages are attached to a binding.

**Exigent circumstances**
- Allows officials to seize evidence before its destroyed (police team fall in)

**Chain of custody**
- Collection, analysis and preservation of data

**Forensics uses bit-level copy of the disk**

**Hacker and crackers**
- want to verify their skills as intruders

**Notebook**
- most preferred in the legal investigation is a bound notebook, pages are attached to a binding.

**Exigent circumstances**
- Allows officials to seize evidence before its destroyed (police team fall in)

**Chain of custody**
- Collection, analysis and preservation of data

**Forensics uses bit-level copy of the disk**

**FBI, DEA, and Secret Service**
- Use similar procedures

**Residual risk**
- Where cost of applying extra countermeasures is more than the estimated loss resulting from a threat or vulnerability (C > L). Legally the remaining residual risk is not counted when deciding whether a company is liable.

**FAIR Information Practices**
- Openness
- Collection Limitation
- Purpose Specification
- Use Limitation
- Data Quality
- Individual Participation
- Security Safeguards
- Accountability
# Physical Security

## Threats
- Natural environment threats (earthquakes, floods, tornadoes)
- Supply system threats (power communications, water, gas)
- Manmade threats (vandalism, fraud, theft)
- Politically motivated threats (terroristic attacks, riots, bombings)

**Life safety takes precedence!**
- Layered defense model: all physical controls should be work together in a tiered architecture (stacked layers)

Vulnerability = weakness threat = someone will identify the weakness and use it against you and becomes the threat agent

Risk analysis -> Acceptable risk level -> baseline -> implement countermeasures

### Major Sources:
- Temperature
- Gases
- Liquids
- Organism: viruses, bacteria
- Projectiles: cars, trucks, bullets
- Movement: collapse, earthquakes
- Energy: radio, radiation

## Controls
- Physical (Fences, Trees, Locks)
- Administrative (badges, clothing procedures)
- Technical (Alarms, Humidity, AC heat controllers)

## Types of Control
- Preventive (guards, dogs, firewall)
- Detective (CCTV, motion detectors, audit logs)
- Corrective (IDS, Antivirus)
- Deterrents (fences, alarms personnel)
- Recover (backup)
- Compensating (monitoring, supervising)

## Electrical Power
### Interference
- **Clean** = no interference
- **Line noise** = can be EMI or RFI
- **Transient** = short duration of noise
- Counter: voltage regulators, grounding/shielding, and line conditioners

### EMI
- **COMMON mode noise** = difference between hot and ground
- **Transverse mode noise** = difference between hot and neutral
- **HINT**: common = grounds

### Excesses
- **SPIKE** = short, high voltage
- **SURGE** = long, high voltage
- Counter: surge protector

### Losses
- **FAULT** = short outage
- **BLACKOUT** = long outage
- Counter: Backup power
- **Long term**: Backup Power generator
- **Short term**: UPS
  - Online uses ac line voltage to charge batteries, power always through UPS
  - Standby UPS, inactive till power down

### Degradation
- **SAG/DIP** = short, low voltage
- **BROWNOUT** = long, low voltage
- Counter: constant voltage transformers

### Other
- **Inrush Surge**: surge of current required to power on devices
- **Common-mode noise**: radiation from hot and ground wires
- **Transverse-mode noise**: radiation from hot and neutral wires.

### Static Charge
- 40 sensitive circuits
- 1000 scramble monitor display
- 1500 disk drive data loss
- 2000 system shutdown
- 4000 Printer Jam
- 17000 Permanent chip damage
- Use antistatic spray and flooring, ground rooms properly

### Humidity
- <40% static electricity up to 20,000 volts
- NORMAL 40-60% up to 4000 volts
- >60% corrosion

## Fire
### Prevention
- Training construction, supplies, reach ability

### Detection
- Manual: pull boxes
- Automatic dial-up: Fire department, aka Auxiliary station alarm
- Detectors:
  - Smoke activated
  - Heat activated
  - Flame activated (infrared)

### Classes
- A: Common WATER, SODA ACID
- B: Liquids—GAS/CO2, SODA ACID
- C: Electrical—GAS/CO2
- D: Metals—DRY POWDER

### Sprinklers
- **Wet pipe**: always contains water, fuse nozzle melts at 165F
- **Dry pipe**: water in tank until clapper valve releases it
- **Deluge**: Douches, large amounts of water/foam
- **Pre-action**: (MOST RECOMMENDED)
  - Water in tanks, first water in pipes when air is lost when heat is detected, then thermal link in nozzle melts to release water

### HALON
- 1211 = portable
- 1301 = flooding
- FM-200 most common replacement (others: CEA, NAF, FE-13, Argon, INERGEN, Low Pressure Water)

### Resistance
- Walls: 1 hour fire rating and adjacent room with paper 2 hours
### Domain 10 - Physical Security

#### Locks
- **Warded lock**: hanging lock with a key
- **Tumbler lock**: cylinder slot
- **Combination lock**: 3 digits with wheels
- **Cipher Lock**: Electrical device lock
- **Preset ordinary door lock**: bolt down hardware
- **Programmable combination or electrical lock**: Raking = circumvent a pin tumbler lock

#### Lightning
- **Glare protection against blinding by lights**
- **Continuous lightning**: evenly distributed lightning
- **Controlled lightning**: no bleeding over no blinding
- **Responsive areas illumination**: IDS detects activities and turns on lightning

NIST: for critical areas the area should be illuminated 8 feet in height with 2-foot candle power

#### Fences
- Small mesh and high gauge is most secure
- 3-4 feet deters casual trespasser
- 6-7 feet to hard to climb easily
- 8 feet + wires deters intruders, no one stops a determined intruder

#### Location
- **CPTED Crime Prevention Through Environmental design**
  - Natural Access control: guidance of people by doors, fences, bollards lighting, security zones defined
  - Natural surveillance: cameras and guards
  - Territorial Reinforcements: walls, fences, flags
- **TARGET HARDENING**: focus on locks, cameras guards
- **FACILITY SITE**: CORE OF BUILDING (thus with 6 stores, on 3rd floor)

FAIL SAFE: doors UNLOCK
FAIL SECURE: doors LOCK

#### CCTV
- **Multiplexer allows multiple camera screens shown over one cable on a monitor**
- Via coax cables (hence closed)
- **Attacks**: replayed (video images)
- Fixed mounting versus PTZ Pan Tilt Zoom
- Accuicnator system (detects movements on screen and alerts guards)
- **Recording (for later review)** = detective control

#### Intrusion detection
**PHYSICAL PARAMETER DETECTION**
- **Electromechanical**: detect a break or change in a circuit magnets pulled lose, wires door, pressure pads
- **Photoelectric**: light beams interrupted (as in a store entrance)
- **Passive infrared**: detects changes in temperature
- **Acoustical detection**: microphones, vibrations sensors

- **MOTION**
  - Wave pattern: motion detectors; detects motions
  - Proximity or capacitance: detector: magnetic field detects presence around an object

#### Audit trails
- **Date and time stamps**
- **Successful or not attempt**
- **Where the access was granted**
- **Who attempted access**
- **Who modified access privileges at supervisor level**

#### Security access cards
- **Photo id card: dumb cards**
- **Digital-coded cards**:
  - Swipe cards
  - Smartcards
- **Wireless proximity cards**
- **User activated**
- **System sensing**
  - Passive device, no battery, uses power of the field
  - Field Powered device: active electronics, transmitter but gets power from the surrounding field from the reader
  - Transponders: both card and receiver holds power, transmitter and electronics

#### ALARMS
- **Local alarms**: audible alarm for at least 4000 feet far
- **Central stations**: less than 10 mins travel time for e.g. an private security firm
- **Proprietary systems**: owned and operated by the customer.
  - System provides many of the features in-house
  - **Auxiliary Station systems**: on alarm ring out to local fire or police

- **Line supervision check** if no tampering is done with the alarm wires
- **Power supplies**: alarm systems needs separate circuitry and backup power

#### Data destruction and reuse
- **Object reuse**: use after initial use
- **Data remanence**: remaining data after erasure
- **Format magnetic media**: 7 times (orange book)

- **Clearing**: overwriting media to be reused
- **Purging**: degaussing or overwriting to be removed
- **Destruction**: complete destroy preferably by burning

#### Other things to know
- **Piggybacking**: looking over someone’s shoulder to see how someone gets access.

- **Data center should have**:
  - Walls from floor to ceiling
  - Floor: Concrete slab: 150 pounds square foot
  - No windows in a datacenter
  - Air-conditioning should have own Emergency Power Off (EPO)

- **Electronic Access Control (EAC)**: proximity readers, programmable locks or biometric systems

- **Order of actions when fire is detected**:
  - Evacuate the facility
  - Shut down computer systems and power if possible
  - Inform facility management contract fire department