CISSP STUDY GUIDE

1. SECURITY MGMT PRACTICES

Topic	Description
Security Management Includes	• Risk Management • Info Security Policies, Procedures, Standards, Guidelines, and Baselines • Information Classification • Security Organization • Security Education **These core components serve as the foundation of a corp. security program**
Security Program	**Goal:** Protect companies Assets ***Mgmt support is one of the most important parts of a security program***
Risk Assessment Will	• Identify Assets • Discover threats that put them at risk • Estimate possible damage and potential loss if threats become real **Results of a Risk Assessment will:** Help mgmt construct a budget to protect the recognized assets from their identified threats and develop applicable security polices that provide direction for security activities.
Security Components can be	1. **Technical** – Firewalls, encryption, and ACLs 2. **Non-Technical** – Security policies, procedures, and compliance enforcement.
Security Mgmt Responsibilities	• **Key during initial security planning process is to define reporting relationships.** **First:** Clear scope needs to be defined and actual goals need to be determined **Second:** Identify company assets, assigning values, and documenting them **Third:** Implementation of security policies, procedures, standards, and guidelines provide integrity, confidentiality and availability for these assets. ***Mgmt responsibilities are to provide protection for resources as in human, capital, hardware, and information forms.** • **Security mgmt has become more important over the years b/c networks have evolved from centralized environments to distributed.**
Roles and Responsibilities	1. **Information Owner** – usually a senior exec within the mgmt group of the company. Has the final Corp responsibility for data and resource protection and would be the one held liable for the negligence when it comes to protecting the company's assets. They are responsible for assigning classifications to info and dictating how the data should be protected. 2. **Security Admin** – job to ensure that mgmt's directives are fulfilled when it comes to security, not to construct the directives. Should be a clear communication b/t Sec Admin and senior mgmt.
Controls	1. **Administrative** – development and publication of policies, standards, procedures and guidelines, screening of personnel, security awareness training, and change control procedures. 2. **Technical (Logical Controls)** – access control mechanisms, password and resource mgmt, identification and authentication methods, security devices, and configuration of the infrastructure. 3. **Physical** – Controlling individual access into facility and different dept., locking systems and removing unnecessary floppy/CD drives, protecting the perimeter of the facility, monitoring for intrusion and environmental controls.
AIC Triad – Critical principals of security	***All security controls, mechanisms, and safeguards are implemented to provide one or more of these capabilities and all risks, threats, and vulnerabilities are measure in their potential to compromise one or all of the AIC principals.** 1. **Availability** – Ensures reliability and timely access to data and resources to authorized individuals. • Systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance • Systems/Networks should be able to recover from disruptions in a secure and quick manner so productivity will not be negatively affected. • Backups should be used • DOS attacks are popular methods of disrupting availability 2. **Integrity** – upheld when the assurance of accuracy and reliability of info and systems is provided, and unauthorized modification of data is prevented. • Environments that enforce this security attribute ensure hackers or mistakes by users do not compromise the integrity of systems or data. • Security should streamline the users' abilities and give them only certain choices and functionality. • Applications should provide mechanisms that check for valid and reasonable input values.

	3. **Confidentiality** – Provides the ability to ensure that the necessary level of secrecy is enforced at each junction of data processing and prevention of unauthorized disclosure • **Shoulder surfing** – when a person looks over another persons shoulder. • **Social Engineering** – tricking another person into sharing confidential info. • Can be provided by encrypting data as its stored and transmitted, network traffic padding, strict access control, data classification, and training personnel.
Security Definitions	1. **Threat** – Any potential danger to info or systems. Someone/something will identify a specific vulnerability and exploit it. • **Threat Agent** – entity that takes advantage of a vulnerability (e.g. hacker, process accessing data that violates security policy, employee making an unintentional mistake). 2. **Exposure** – an instance of being exposed to losses from a threat agent. A vulnerability can cause an org to be exposed to possible damages. 3. **Vulnerability** – the absence or weakness of a safeguard that could be exploited. 4. **Countermeasure** – or safeguard, mitigates the potential risk by eliminating the vulnerability or reducing the risk of a threat agent exploiting a vulnerability. 5. **Risk** – Probability of a threat agent taking advantage of a vulnerability. • Reducing the vulnerability or the threat reduces the risk • Risk left over after applying countermeasure is residual risk ***CISSP looks at in this order because you have a threat but unless you are exposed to it, it is not really a vulnerability. If you have a vulnerability then you apply the right countermeasure to reduce the risk**
Top down approach to building a security program.	**Top Down Approach -** Security program should use a top down approach, meaning that the initiation, support, and direction come from top mgmt and work their way through middle mgmt and then to staff members. **Top down approach makes sure that the people responsible for protecting the companies assets are driving the program.** **Steps** 1. Process should start with very broad terms and ideas that work its way down to detailed configuration settings **(Security Policy)** 2. Develop and implement procedures, standards, and guidelines that support the security policy 3. Increase granularity by developing standards and configurations for the chosen security controls and methods. **Bottom-up Approach** – If the IT dept tried to develop a security program without getting proper mgmt support and approval. Usually less effective, not broad enough, and doomed to fail.
Security Model	- A framework made up of many entities, protection mechanisms, logical and physical components, procedures, and configurations that all work together in synergistic way to provide a security level for an environment. - Each model is different, but all models work in layers: one layer providing support the layer above it and protection for the layer below it. - **Goal of a security model is assurance**, which is the sum total of all security components within an environment that provide a level of confidence. - Security model a company chooses depends on the type of business, its critical missions, and objectives. **Goals:** 1. **Operational Goals** – Are daily goals, which focus on productivity and task orient activities. 2. **Tactical Goals** – Mid term goals – take more time and effort to complete. 3. **Strategic Goals** – Long term goals. This approach to planning is called the **Planning Horizon** **Assurance** – degree of confidence that a certain security level is being provided.
Private Industry vs. Military Org.	- Security model an org chooses depends on its critical missions and business requirements. **Private Industry** – Out of the AIC triad data integrity and availability usually rank higher. **Military Org.** – Confidentiality ranks the highest.
Risk Mgmt	**Def.** – the process of identifying, assessing, and reducing this risk to an acceptable level and implementing the right mechanisms to maintain that level of risk. • Goal is to assess risks and threats occurring and then reducing the overall level of risk to what the org identifies as acceptable and maintaining that level.
Categories of Risk	1. **Physical damage** – fire, water, vandalism, power loss, and natural disasters. 2. **Human error** – accidental or intentional action or inaction that can disrupt productivity. 3. **Equipment malfunction** – failure of systems and peripheral devices 4. **Inside and outside attacks** – Hacking, cracking, and attacking

	5. **Misuse of data** – sharing trade secrets, fraud, espionage, and theft. 6. **Loss of data** – intentional or unintentional loss of info through destructive means 7. **Application error** – computation errors, input errors, and buffer overflows.
Risk Analysis	**Def –** a tool for risk mgmt – is a method of identifying risks and assessing the possible damage in order to justify security safeguards. • Helps companies prioritize there risks and identifies the amount of money that could be applied to protecting against those risks. • Helps integrate the security program objectives with the company's business objectives and requirements • Helps draft a proper budget for a security program • Needs to be supported by upper mgmt. **4 main goals of a risk analysis:** 1. **identify assets and their threats** 2. **Quantify the business impact of these potential threats** 3. **calculate the risk** 4. **provide an economic balance b/t the impact of the risk and the cost of the countermeasure** **Cost/Benefit Analysis** – provided by risk analysis – where the annualized cost of safeguards to protect against the threats is compared with the expected loss. • **Safeguard should not be implemented unless the annualized cost of the loss exceeds the annualized cost of the safeguard.**
Risk Analysis Team	- a team needs to be built with individuals from many or all of the departments to verify that all risks are identified and addressed
Value of an asset	- Actual value is determined by the cost it take to acquire, develop, and maintain it. - The value of an asset is determined by the importance it has to the owners, authorized, and unauthorized users. - Value of an asset should reflect all identifiable costs that would arise if there were an actual impairment of the asset.
Identifying threats	**Illogical Processing** – if the inputted data is incorrect or values to calculate are incorrect. **Cascading Errors** – invalid results are passed on to another process **Loss Potential** – what the company would lose if a threat agent actually exploits a vulnerability. **Delayed Loss** – Negative effects on a company after a vulnerability is initially exploited. Need to be looked at when performing a risk analysis.
Quantitative Approach	**Def** – attempts to assign real and meaningful numbers to all elements of the risk analysis process. • Expressed in dollar amts and percentages. • Provides concrete probability percentages when determining the likelihood of threats and risks. • All elements within the Analysis **(asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items)** is quantified and entered into equitation's to determine total and residual risks. ***Purely quantitative risk analysis is not possible because the method is attempting to quantify qualitative items and there will always be uncertainties.**
Steps of a Risk Analysis	1. Assign value to info and assets 2. Estimate potential loss per risk • Calculate **SLE** – Single Loss Expectancy **–** dollar amount assigned to a single event that represents the companies potential loss amt if a specific threat took place. **SLE = Asset Value X Exposure Factor (EF)** • **Exposure Factor** – Percentage of asset loss caused by identified threat. 3. Perform a threat analysis • Includes Calculating the **ARO** – Annualized Rate of Occurrence – Estimated frequency a threat could happen in a year. • **ARO range can be from 0.0 (never) to 1.0 (always)** 4. Derive the overall loss potential per threat • Calculate **ALE** – Annualized Loss Expectancy – Tells the company that if they want to put in controls/safeguards to protect the asset from a threat they should only spend this amount. **ALE = SLE X ARO** 5. Reduce, assign, or accept risk a. **Reduce** – Countermeasures b. **Assignment or Transfer** – Buy insurance c. **Accept** – Live with. d. **Reject –** Dangerous, when a company is in denial or ignores it.
Results of a Risk Analysis	• Assigned monetary values assigned to assets

	• Comprehensive list of all possible and significant threats • Probability of the occurrence rate of each threat • Loss potential the company can endure per threat in a year time span • Recommended safeguards, countermeasures, and actions
Qualitative Risk Analysis	**Def** – no assigned values, instead walk through different scenarios of risk possibilities and reank the seriousness of the threats and the validity of the different countermeasures. • Qualitative rating would be expressed in high, medium, low or on a scale of 1 to 5 or 1 to 10. **Examples of Qualitative Techniques:** 1. **Delphi** – a group decision method designed to ensure that each member gives an honest opinion. Each member writes down his or her opinion of a risk on a piece of paper. Results are compiled and distributed to the members who write down their comments anonymously. Process continues until a consensus is formed. **Anonymously** 2. **Brainstorming** 3. **Storyboarding** 4. **Focus Groups** 5. **Surveys** 6. **Questionnaires** 7. **Checklists** 8. **One-on-One Meetings** 9. **Interviews.**
Qualitative vs. Quantitative	• Risk analysis team, mgmt, risk analysis tools, and culture will dictate the approach. **Quantitative:** • Requires more complex Calculations • Easily automated • Provides a cost/benefit analysis • Uses independent and objective metrics • Shows clear cut losses that can be accrued within 1 year. **Qualitative:** • Degree of guesswork involved • Provides the opinions of the staff that knows the processes best.
Countermeasure Selection	**AKA – Safeguard** • Good countermeasure must be cost-effective and that its benefit outweighs its cost. • Should default to least privilege, have fail-safe defaults, and override capabilities. • Should be imposed uniformly so everyone has the same restrictions and functionality. Use a **Cost/Benefit Analysis:** **Value of safeguard to the company = [ALE before implementing safeguard] – [ALE after implementing safeguard] – [Annual cost of safeguard]**
Total Risk vs. Residual Risk	**Residual Risk** – Risk left over after it has been mitigated. • **Residual Risk = (Threats X Vulnerability X Asset Value) X Controls Gap** **Total Risk** – Risk if no mitigation has taken place. • **Total Risk = Threats X Vulnerability X Asset Value**
Policies, Procedures, standards, baselines, and guidelines	• Senior mgmt needs to determine what is to be expected from employees and what the consequences of noncompliance will be. • Security program and policies should have long-term security strategy. • Security program should have policies, procedures, standards, baselines, guidelines, security awareness training, incident handling, and a compliance program. HR and Legal should be involved in the development. • **Should not be in one document. Being separate and modular helps for proper distribution and updating.**
Security Policy	**Def** – a general statement produced by senior mgmt to dictate what type of role security plays within the org. Security policy can be an Org policy, issue-specific policy, or system-specific policy. • **Org Security Policy** – mgmt est. how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines enforcement. Policy must address laws, regulations, and liability issues. • Provides scope and direction for all future security activities within the org and the amt of risk senior mgmt is willing to accept. • **Issue-Specific Policy** – Also called functional implementing policies – address specific security issues that mgmt feels need more detailed explanation and

	attention to. (i.e. email policy). Provides direction and structure for the staff including what they can and cannot do. Outlines expectations of actions and provides liability protection. • **System-Specific Policy** – Presents mgmt decisions that are closer to the actual computers, networks, applications, and data. (i.e. approved vendor list, DB protection, firewalls & IDS are deployed etc.) **Types of Policies:** 1. **Regulatory** – ensure that the org is following standards set by a specific industry and is regulated by law. 2. **Advisory** – Written to strongly suggest certain types of behaviors and activities that should take place within the org and consequences. 3. **Informative** – Written to inform employees of certain topics. Not enforceable. *Policies are broad overview terms to cover many subjects in a general fashion. PROVIDES THE FOUNDATION, procedures, standards, and guidelines provide the security framework.
Standards	**Def.** Specify how HW and SW products are to be used, expected user behavior. Also ensure specific technologies, applications, parameters, and procedures are carried out in a uniformed way across the org. **Standards, guidelines, and procedures are the tactical goals. Policies are the strategic goals.**
Baselines	**Def** – provides the minimum level of security necessary throughout the Org. Most of the time, baselines are platform unique security implementations.
Guidelines	**Def** – Recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply. • Standards are mandatory rules, Guidelines are general approaches (cover gray areas) that provide the necessary flexibility for unforeseen circumstances.
Procedures	**Def** – detailed step-by-step tasks that should be performed to achieve a certain security goal. • Lowest level in policy chain b/c they are closest to the computers and users and provide detailed steps for config and installation issues. • Spell out how policy, standards, and guidelines will be implemented. • Should be detailed enough to be able to be understood and used by a diverse group of individuals.
Due Diligence and Due Card	**Due Diligence** – act of investigating and understanding the risks the company faces. Understanding the current threats and risks. **Due Care –** Shows a company has taken responsibility for the activities that take place within the Corp. A company shows by developing security policies, procedures, and standards and implementing countermeasures.
Information Classification	**Purpose** – to indicate the level of confidentiality, integrity, and availability that is required for each type of info. • Also helps to ensure that data is protected in the most cost effective manner. • Each sensitivity classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.
Private Business vs. Military Classifications	**Private Business Classifications:** **1. Confidential** **2. Private** **3. Sensitive** **4. Public** **Military Classifications:** **1. Top Secret** **2. Secret** **3. Confidential** **4. Sensitive but unclassified** **5. Unclassified**
Data Classification Procedures/Steps	1. Identify data custodian who will be responsible for maintaining data and its security level. 2. Specify the criteria that will determine how data is classified 3. The data owner must indicate the classification of the data they are responsible for. 4. Indicate the security controls that are required for each classification level. 5. Document any exceptions to the previous classification issues. 6. Indicate the methods that can be used to transfer custody of the info to a different data owner. 7. Indicate termination procedures for declassifying the data. 8. Integrate these issues into the security awareness program so that all employees understand

	how to handle data at different classification levels.
Senior mgr	Ultimately responsible for security of the org and protection of its assets
Security Professional	Functionally responsible for security and carrying out senior manager's directives.
Data Owner	**Def** – Usually a member of senior mgmt and is ultimately responsible for the protection and use of a specific subset of info. • Determines classification level and responsible for alteration of classification levels if need arises. • Delegates responsibility of day to day maintenance to Data Custodian
Data Custodian	**Def** – responsibility of maintenance and preserving/protection data confidentiality, integrity, and availability. • Usually filled by System Administrator and duties include: • Backups of data • Implementing security mechanisms • Validating integrity of data • Restoring data from backups • Fulfilling requirements specified in the company's security policy, standards and guidelines. **System Admin** – Responsibility of individual devices/computers **Network Admin** – Responsibility of how computers and devices are connected and work together w/in a network.
User	**Def** – Uses data for data processing tasks. • Users must have the necessary level of access to the data to perform the duties.
Separation of Duties	**Def** – makes sure that one individual cannot complete a critical task by themselves. Would take collusion.
Collusion	**Def –** at least 2 people would need to work together to cause some type of destruction or fraud.
Hiring Practices	**Non-disclosure Agreements** - need to be developed and signed by new employees to protect the company and its sensitive info. • Reference should be checked, education verified, drug/background checks done **Job Rotation** – Rotation of employees from one position to another. Prevents too much control of a segment of the business by an individual. Prevents fraud, data modification, or Info misuse.
Security Awareness	- Communication of security program to employees. - Should be comprehensive, tailored to specific groups, and organization-wide - Expected responsibilities and acceptable behaviors need to be clarified and noncompliance repercussions that could range from a warning to dismissal need to be explained before being invoked. **Different types of Security Training:** 1. **For Management –** Benefit from a short, focused security awareness orientation that discusses corporate assets and financial gains and losses pertaining to security. • **For Mid-Mgmt** – benefit from more detailed explanations of the policies, procedures, standards, and guidelines and how map to individual departments. 2. **For Technical Departments** – More in-depth training to discuss technical configurations, incident handling, and indications of different types of security compromises. 3. **For Staff members** – Understand why security is important to the company and import to them individually. Includes examples of acceptable and unacceptable activities. • **Each group** needs to know whom it should report suspicious activity to and how they are expected to handle situations. • Security training should be done once a year. • **Main reason for Security Awareness Training is to modify employees' behavior and attitude toward security.**
Objectives of loss prevention program	- reduce losses to a predefined level of tolerance.

2. Access Control

Topic	Description
Access Controls	**Def –** Security features that control how users and systems communicate and interact with other systems and resources. • Protect the systems and resources from unauthorized access. • **Extremely Imortant b/c** it is one of first lines of defense used to fight against unauthorized access to systems and network resources.

	- Give an org the ability to control, restrict, monitor, and protect resource AIC.
Access, Subject, & Object	**Access** – The flow of info b/t a **subject** and an **object**. **Subject** – an **active** entity that requests access to an object or the data w/in an object. Subject can be a user, program, or process that accesses an object to accomplish a task. **Object** – A **passive** entity that contains info. Can be a computer, DB, File, computer program, directory or field contained in a table w/in a DB
3 Security Principals	1. **Availability** – Information is accessible and available for users when it is request so they can carry out tasks and fulfill responsibilities. - Fault tolerance and recovery mechanisms are in place to ensure continuity of availability. - **Information has various attributes** such as accuracy, relevance, timeliness, and privacy. 2. **Integrity** – When a security mechanism provides integrity it will protect data from being altered in an unauthorized fashion. - If some type of illegitimate modification does occur, the security mechanism must alert the user or discard the message altogether. 3. **Confidentiality** – Assurance that info is not disclosed to unauthorized individuals, programs, or processes. - Control mechanisms need to be in place to dictate who can access data and what the subject can do with it once it has been accessed. These activities should be **controlled, audited, and monitored.** - Some security mechanisms that provide confidentiality are encryption, logical and physical access controls, transmission protocols, DB views, and controlled traffic flow.
Identification, Authentication, Authorization, and Accountability	**Identification** – method of ensuring that a subject (user, program, process) is the entity it claims to be. Can be provided with use of username or account number. Entering public information. **Authenticated** – subject is required to provide a second piece to the credential set. Could be a password, passphrase, cryptographic key, PIM, anatomical attribute, or token. Entering Private information. - Once the credentials are matched against stored info the subject is **authenticated.** **Authorized** – If the subject can access a resource. - **To ensure accountability** the subject must be uniquely identified and the subjects actions are recorded. **Logical Access Controls** – Tools used for identification, authentication, authorization, and accountability. **Logical and Technical controls can be used interchangeably on the test.**
3 Factors for Authentication	1. **Something a person knows** – password, Pin Etc. - Least expensive to implement - Easily subverted by an attacker compared to the other two. 2. **Something a person has** – Key, swipe card, token etc. - If item is lost or stolen unauthorized user can gain access. 3. **Something a person is** – Biometrics (fingerprint, thumbprint, retina scan etc.) - Most expensive solution - Least likely to be subverted by an attacker. **Strong Authentication or 2 factor authentication** – Use of two or more of the factors for authentication.
Biometrics	**Def** – verifies an individuals identity by a unique personal attribute, which is on of the most effective and accurate methods of verifying identification. **Type I Error** – When a biometric system rejects and authorized individual. **Type II Error** – When the system accepts imposters who should be rejected **CER** – Crossover Error Rate – Represents the point at which the false rejection rate equals the false acceptance rate and is expressed in a percentage. AKA when Type I Errors = Type II Errors. - If you lower the Type II error rate you will increase the Type I and vice versa. - Example: A CER = 3 will be more accurate than a system with a CER = 4
Types of Biometric Scanning devices	1. **Fingerprint** – Fingerprints are made up of ridge endings and bifurcations exhibited by the friction ridges and other detailed characteristics that are called **minutiae.** - Fingerprint systems store the full fingerprint, which takes up a lot of memory. - **Finger-scan** technology extracts specific features from the fingerprint and stores just that info. Takes up less memory and allows quicker DB lookups and comparisons.

	2. **Palm Scan** – Stores palm information and each fingerprint info. 3. **Hand Geometry** – Size and width of a persons hand and fingers is analyzed and stored. 4. **Retina Scan** – Reads a persons retina and scans the blood vessel pattern of the retina on the backside of the eyeball. 5. **Iris Scan** – Colored portion of the eye. Has unique patterns, rifts, colors, rings, coronas, and furrows. Captured and stored. Scanner needs to be placed in a non-sunlight area for it to work correctly. 6. **Signature Dynamics** – Usually a person signs the same manner and speed each time. Signing produces an electrical signal that is analyzed and captured by the biometric system. • Captures the speed of signing, the way the person holds the pen, pressure generated when signing. 7. **Keyboard Dynamics** – Captures electrical signals when a person types a certain phrase. • When a person types a specified phrase the biometric captures speed and motions of the action. 8. **Voice Print** – Individual repeats a certain phrase, it is stored and compared. 9. **Facial Scan** 10. **Hand Topology** – Takes a side view picture of the hand and looks at peaks and valleys of the hand along with shape and curvature.
Password Mgmt	• Most commonly used authentication mechanism and the weakest. • If a password generator is going to be used, the tools should create pronounceable non-dictionary words to help users remember them and not be too complicated to cause the user to write them down. **Clipping Level** – failed logon attempts setting. Protects against dictionary and brute force attacks. **Attacks to gain passwords:** 1. **Electronic Monitoring** – listening to network traffic and taking user password 2. **Accessing Psswd file** 3. **Brute Force Attacks** 4. **Dictionary Attacks** 5. **Social Engineering**
Password Checkers vs. Crackers	**Password Checker** – a tool used by a Security Professional to test the strength of passwords **Password Cracker** – a tool used by an attacker to obtain access to the system
Cognitive Passwords	**Def** – Fact or opinion based info used to verify an individuals identity. A user is enrolled by answering several questions based on life experiences. Authentication will then ask her these questions instead of remembering a password. • Best for a service the user does not use on a daily basis b/c it is longer than other authentication mechanisms • Works well for help desk when identifying an individual
One-time Passwords	**Def** – also called a dynamic password. It is used when a user needs to authenticate themselves and can only be used once. • Used in environments that require a higher level of security **2 Types of one-time password token generators:** 1. **Synchronous** 2. **Asynchronous**
Token Device and Synchronous vs. Asynchronous	**Token Device** – password generator, usually a handheld device that has an LCD display. The token device and authentication service need to be synchronized in some manner to be able to authenticate the user. **Synchronous Token Device** – synchronizes with the authentication service by using time or an event as the core piece of the authentication process. **Which ever Synchronous being used the authentication server and token need to share the same secret key.** • **Time Based Synchronous** – token device and the authentication service must hold the exact same time within their internal clocks. Time value on the token device is encrypted with a secret key and present to the user. User enters on to the system, authentication server decrypts, compares the two values. • **Event-Synchronous** – User needs to initiate the logon sequence on the computer and push a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. **Asynchronous Token Device** – uses a challenge response scheme to authenticate the user. The computer the user is attempting to log onto displays a challenge value to the user that it received from the authentication service. The user

	types this value into the handheld token and the token encrypts this value and presents the new value to the user who then types it and an ID into the computer. **Disadvantages of Token Device:** • Vulnerable to masquerading if user shares his ID or username along with the token device. • Battery failure of token can restrict successful authentication **Advantages**: • Not vulnerable to electronic eavesdropping, sniffing, or password guessing.
Cryptographic Keys for Identification – Private Key or Digital Signature	**Private key** – a secret value that should be in the possession of one person and not be disclosed to an outside party. **Digital Signature** – uses a private key to encrypt a hash value (message digest). • The act of encrypting this hash value with a private key is called **digitally signing a message.** • A digital signature attached to a message proves that the message originated from a specific source and the message was not changed in transit.
Passphrase	**Def.** – used for authentication – a sequence of characters that is longer than a password. The user enters this phrase into an application and the application transforms the value into a **virtual password**. • Stronger than a password because it is longer • Easier to remember than a password. • Drawback, takes longer to enter into the system during authentication
Memory Cards and Smart Cards	**Memory Cards** – holds information, but does not process info. • Can hold a user's authentication info, so this user only needs to type in a user ID or PIN, present the memory card, and if the two match an are approved by an authentication service, the user is successfully authentication. • Most cases ID data is pulled from memory card to authentication engine (i.e. ATM card) **Smart Card** – has the necessary HW and logic to actually process the info. • Can provide two-factor authentication b/c a user may need to enter a PIN to unlock the smart card. • To authenticate using a smart card, user inserts card into a reader and enters a PIN. The reader performs a one-way hash on the PIN and stores it in the memory of the card reader. Reader than performs the same one-way hash on the info on the smart card and compares the 2 values. • Authentication to the computer can be in the form of a one-time psswd, use of challenge/response value, or by providing the user's private key if used w/in a PKI environment. • Info on a smart card is not readable until the correct PIN is entered. This fact and complexity of the smart token make them resistant to reverse-engineering. • Also can be programmed to store encrypted info, detect any tampering of the card. If tampering is detected info can be automatically deleted. • Downfalls – extra cost of readers and the overhead of card generation. Smart cards more expensive the memory cards.
Access Criteria	• Granting access rights to subjects should be based on the level of trust a company has in a subject and the subjects need to know. **Access Criteria Types:** 1. **Roles** – based on a job assignment or function. 2. **Groups** – Placing users that all need the same access into a group. 3. **Physical or Logical Location** – Physical – i.e. requiring users to only log on from the console. Logical – usually done through network address restrictions. 4. **Time of Day or Temporal Isolation** 5. **Transaction Type** – control what data is accessed during certain types of functions and what commands are carried out on the data. • **Access control mechanisms should default to no access.** Which means if access is not explicitly allowed it should be implicitly denied (ACL's)
Need-to-Know Principle	- Individuals should only be given access to the info that they absolutely require in order to perform their job duties. - **Its mgmt job to determine the security requirements of individuals and how access is authorized.** - Admin and IT staff configure the access control and the security officer configures the security mechanisms to fulfill these requirements, but not job to determine security requirements of users.
Single Sign-on	**Def.** – allows a user to enter credentials one time and be able to access all resources in primary and secondary network domains. **Advantages**

	• Reduces the amt of time users spend authenticating to devices • Gives the admin the ability to streamline user accounts and have better control over access rights. • Improves security by reducing the probability of users writing down passwords • Reduces the admin time on adding and removing user accounts and modifying access permissions. If an admin needs to disable or suspend an account, it can be done uniformly. **Disadvantages:** • Interoperability issues with different platforms • Once an attacker is in they get access to all systems
Single Sign-on Technologies	**Scripting** – Most simplistic and consists of writing batch files and scripts that contain each user ID, password, and logon commands necessary for each platform. Runs in the background. • Demands a lot from the Admin, if a user changes any information it needs to be updated in all scripts • Scripts must be stored in a protected area. **Kerberos** – An authentication protocol designed by MIT in the Mid-80's as part of the Athena Project. • Uses symmetric key cryptography and provides end-to-end security. • Although it allows the use of passwords for authentication, it was designed specifically to eliminate the need for transmitting passwords over the network using cryptography keys and shared secret keys. • Provides confidentiality of data by encryption and access controls to resources. Does not protect a computers or services availability. **SESAME** – access control technology developed in Europe and based on Public key cryptography. **Thin Clients** – Dumb terminals authenticating to a server or mainframe. **Directory Services** – Network aware services that control access to resources.(i.e. LDAP, NDS, and AD)
Main Components In Kerberos	**KDC** – Key Distribution Center **– The most important component** – Holds all the users' and services' cryptographic keys. • Provides authentication services, as well as key distribution functionality • Clients and services trust the integrity of the KDC and this trust is the foundation of Kerberos security. • KDC provides security services to entities referred to as **Principals –** users, applications, services. • KDC and each principal share a secret key. KDC maintains a DB w/ identify information on all principals and secret keys. • **Ticket** – generated by the KDC and given to a principal when the principal needs to authenticate to another principal. • **Realm** – a set of principals a KDC provides security services for. Once KDC can be responsible for one or several realms. Realms allow an Admin to logically group resources and users. • **AS** – Authentication Service – Part of KDC that authenticates the principal • **TGS** – Ticket Granting Service – Part of KDC that makes the tickets and hands them out to the principals
Kerberos Authentication Process	1. Some wants to print 2. Kerberos client on the computer prompts the user for a user ID. User ID gets sent to the KDC along with the name of print service requested. 3. The Ticket Granting service receives the request and verifies user and print service are in its DB. If both are the KDC provides a session key for the user and print service to use. One instance of the session key is encrypted with the service's secret key and the other instance of the session key is encrypted with users secret key. Encryption verifies it came from KDC. 4. KDC generates a service ticket that holds both instances of the session key and it is sent back to the client SW on users computer. Client software prompts the user for a password, its entered, and the client converts it into the key that is necessary to decrypt the session key within the ticket. 5. Client SW decrypts the users portion of the ticket and gives the user a copy of the session key and sends the ticket onto the print service to authenticate the user. Print service uses its secret key to decrypt the ticket and now has a copy of the session key. 6. The user is now authenticated to the print services and the session key is used to encrypt/decrypt messages. User can now print. • If Kerberos implementation is configured to use an **authenticator** the user will send the print server there identification info and a time stamp encrypted with the session key they share. Print server will decrypt and compare the ID data the KDC sent to it about the requesting user. Time stamp is used to help fight replay attacks

	• Tickets have a time limit, that is configurable by the Admin, but is usually 1 day.
Weaknesses of Kerberos	• KDC is a single point of failure • KDC must be robust enough to handle the number of requests • Secret keys are temporarily stored on the users workstations, possibility for an attacker to obtain. • Session keys are decrypted and reside on the user on the users workstation • Kerberos is vulnerable to password guessing. Does not know a dictionary attack is occurring. • Network traffic is not protected by Kerberos if encryption is not enabled. • When a user changes their password, it changes the secret key and KDC DB needs to be updated.
SESAME	**Secure European System for Applications in a Multi-Vendor Environment** – A project of single sign-on technology to extend Kerberos functionality and improve its weaknesses. **Based on public key cryptography.** • Uses symmetric and asymmetric cryptographic techniques to protect exchanges of data and to authenticate subjects to network resources (Kerberos only uses symmetric). • Instead of Tickets SESAME uses **PACs** – Privileged Attribute Certificates – contains the subjects identity, access capabilities for the object, access time period, and lifetime of PAC. PAC is digitally signed so that the object can balidate that it came from the trusted authentication server, which **is PAS –** Privileged Attribute Server.
Access Control Models	**Def** – a framework that dictates how subjects access objects. Uses access control technologies and security mechanisms to enforce the rules and objectives of the Model. **3 types:** 1. **Discretionary** 2. **Mandatory** 3. **Nondiscretionary (role-based)** ***Business and security goals of an org will help prescribe what access control model should be usedB**
DAC	**Discretionary Access Control** – enables the owner of the resource to specify which subjects can access specific resources. Called discretionary b/c the control of access is based on the discretion of the owner. • If a user creates a file, they are the owner of the file and would be able to set permissions to access. • Most common DAC is using ACL's – which are dictated and set by the owners and enforced by the OS. • Used by Windows, Macintosh, and most Unix. • System compares the subjects permissions and rights to the ACL on the resource. • Used if does not require high level of security.
MAC	**Mandatory Access Control** – Much more structured and strict and is based on security label system. • Operating system makes the final decision and can override the data owners wishes. • Users are given a security clearance and the data is classified in the same way. Classifications are stored in the security labels of the resources • Rules for how subjects access data are made by mgmt, configured by Admin, enforced by the OS and supported by security technologies. • Type of model is used in environements where info classification and confidentiality is of utmost importance (military). • SE Linux is a MAC system developed by NSA and Secure Computing. • System makes access decisions by comparing a subjects clearance and need to know to that of the security label **Security Labels** – When MAC is used every subject and object must have security labels which contain a classification and different categries. • Classifications – (top secret, secret, etc) • Categories **–** enforces the need-to-know rules. Just because someone has top secret clearance does not mean they need to know all top secret info.
RBAC	**Role Based Access Control or Nondiscretionary Access Control** – A centrally administered set of controls to determine how subjects and objects interact. Allows access to resources based on the role the user holds within the company. • Owners decide what privileges to assign to the roles and what users to assign those roles. • Admin creates the roles and functions within the systems that they are maintaining on behalf of the owners. • Security Admin actually adds the privileges to the user IDs and groups. • Using roles any user assigned to that role only has the rights of that role. • Best for companies that have high employee turnovers.

	• Used if does not require high level of security. **RBAC can use:** 1. **Role-based** – role of the user within the company. 2. **Task-based** – determined by the task assigned to this user. 3. **Lattice-based access** – determined by the sensitivity level assigned to the role. • Variation of Nondiscretionary access control and provides upper and lower bounds of access capabilities for each subject and object relationship. • Subjects have the least upper bound and greatest lower bound of access to labeled objects based on their clearances or assigned lattice position.
Access Control Techniques and Technologies	1. **Rule-based Access Control** – Based on specific rules that indicate what can and cannot happen to an object. Used by routers and FW where the Admin sets the rules and user cannot modify these controls. Authentication service does not take identity into account 2. **Constrained User Interfaces** – Restrict users access abilities by not allowing them to request certain functions or info, or have access to specific system resources. **3 Types of Restricted Interfaces:** a. **Menus and Shells** – users are only given the options of the commands they can execute. b. **Database Views** – used for restricting user access to data that is contained in the DB by configuring a DB so users cannot see field that the DB Admin wants to keep secret. c. **Physically Constrained Interfaces** – Can be implemented by only providing certain keys on a keypad or touch buttons on a screen. 3. **Access Control Matrix** – A table of subjects and objects indicating what actions individual subjects can take upon individual objects. • Matrices are data structures the programmers implement as table lookups that will be used and enforced by the OS. • Usually an attribute of DAC and access rights can be assigned to the subjects (**Capabilities**) or the objects (**ACLs)**. 4. **Capability Tables** – Specifies the access rights a certain subject possesses pertaining to specific objects. • Subject is bound to the capability table like an object is bound to an ACL. • Capability corresponds to the subjects row in the Access control matrix. • Kerberos is a capability-based system. 5. **ACLs** – lists of subjects that can access a specific object and level of authorization granted. Authorization can be specified to an individual, role, or group. i. Maps to the object ii. Corresponds to a column of the matrix. 6. **Content-dependent Access Control** – Access to objects is determined by the content within the object, not solely on subject identity.
Access Control Administration	1. **Centralized** 2. **Decentralized** 3. **Hybrid of the two**
Centralized Access Control Administration	**Def.** – one entity (dept or individual) is responsible for granting all users access to resources. • Mgmt determines how users and resources interact • This entity configures the mechanisms that enforce access control, process any changes that are need to a user profile, disables access, and completely removes rights. • Provides consistent and uniform method of controlling users' access rights. • **Disadv** – slow b/c changes must be processed by one Entity
Examples of Centralized access control technologies	1. **RADIUS** – Remote Authentication Dial-in User Service – authentication protocol that authenticates and authorizes users, usually dial-in. • Only works with PPP and SLIP connections and can only authenticate computers/laptops that use modems and regular authentication protocols as in PAP, CHAP, and EAP. 2. **TACACS** – Terminal Access Controller Access Control System – client server protocol that provides the same time of functionality as RADIUS • Allows credentials to take the form of username and passwords, Kerberos tickets, or security tokens. • RADIUS is an Internet standard and TACACS is a Cisco proprietary protocol. 3. **Diameter** – Authentication protocol developed to work with IPSec if network layer security and encryption are required.

CISSP STUDY GUIDE

Decentralized Access Control Admin	**Def** – gives control of access to the people closer to the resources. **Adv:** • Changes happen faster b/c not just one entity is making changes. **Disadv:** • Different managers may practice security and access controls in a different way • Not consistent controls. • Consistency relating to the companies protection (not removing terms)
Hybrid Access Control Admin	**Def** – Combo of Centralized and Decentralized Access Control Admin. **Admin controls which subjects can access objects w/in the environment and data owners can control which subjects can access the resources they are responsible for.** • Centralized is used for sensitive types of services (domain logon, system file access, DB access) • Decentralized is users can determine who can access individual files and directories they have created.
3 Types of Access Control	1. **Administrative** 2. **Physical Controls** 3. **Technical Controls**
Administrative	- Senior mgmt decides how security will play a role. - First piece is security policy - Work at the top layer of a hierarchical access control model 1. **Policy and procedures** – Security policy is a high level plan stating mgmts intent on practicing security within the company and risks levels willing to accept. 2. **Personnel Controls** – Security controls when a person is hired, terminated, suspended, moved to a different dept, or promoted. Separation of duties, rotation of duties. 3. **Supervisory Structure** – Hierarchical structure of the business that helps fight fraud and enforce proper access control. 4. **Security Awareness Training** 5. **Testing** – Testing all security control mechanisms and procedures on a periodic basis to ensure align with mgmt expectations.
Physical Controls	1. **Network Segregation** – Via physical or logical means. Servers in one area, mainframes in another with controls in place to access only what is needed. 2. **Perimeter Security** 3. **Computer Controls** – locks on laptops, removal of floppy/CD drives, protection device that reduces the electrical emissions. 4. **Work Area Separation** – Only particular individuals can access certain sections of the facility. 5. **Data Backups** 6. **Cabling** – types of cabling limit unauthorized monitoring. Location.
Technical Controls	**AKA Logical Controls** • Protect the integrity and availability of resources by limiting the number of subjects that can access them and protect the confidentiality by preventing disclosure to unauthorized subjects. 1. **System Access** – Enforces access control objectives. 2. **Network Architecture** – Logically segmenting a network. 3. **Network Access** – Controlling access to network areas/segments. via Routers, switches, firewalls, etc. 4. **Encryption and Protocols** – protect info as it passes through a network and resides on computers. 5. **Control Zone** – Combo of technical and physical controls. Area that surrounds and protects network devices that emit electrical signals. 6. **Auditing** – Tools that track activity within a network, on a network device, or specific computer
6 functionalities of Access Controls	1. **Preventative** 2. **Detective** 3. **Corrective** 4. **Deterrent** 5. **Recovery** 6. **Compensating** ***Most productive to use a preventive model and then use detective, recovery, and corrective to help support the model.**
Locks	- Considered delay mechanisms because they will only delay a determined intruder. Goal is delay enough to allow law enforcement or security to respond.
3 types of Audit Trail	1. **Audit reduction** – Tool discards mundane task info and records system performance, security,

Analysis Tools	and user functionality info. 2. **Variance-Detection** – monitors computer and resource usage trends and detect variations. 3. **Attack Signature-Detection** – Application will have a database of info that has been known to indicate specific attacks.
Keystroke Monitoring	**Def** – a type of auditing that can review and record keystrokes entered by a user during an active session. • User of the keystroke tool can either view the characters as they are typed or have the characters written to an audit log to be reviewed at a later time.. • Usually only done for special cases and for a specific amount of time b/c of the amt of info captured can be overwhelming. • Can be privacy issues – need to have this stated in the security policy, addressed in security awareness training, and a banner notice displayed.
Protecting Audit Data and Log info	**Scrubbing** – deleting specific incriminating data w/in audit logs. • Integrity of data can be ensured with the use of digital signatures, message digest tools, and strong access controls. • Confidentiality can be protected with encryption and strong access controls. • **Write-once Media** – to prevent losing or modification of data. • Can be used in trial to prove and individuals guilt, demonstrate how an attack was carried out, or corroborate a story.
Object Reuse	**Def** – Before someone uses a hard drive, floppy disk, or tape it should be cleared of any residual info that was on it previously. • Also applies to objects that are reused by computer process, such as memory locations, variable, and registers. • Formatting a disk or deleting files only removes the pointers to the files, does not remove them until they are overwritten with info. • Before allowing one subject to use media it should be erased, degaussed, or formatted. • Most effective way is to physically destroy the media. • A form of data hiding is to configure a sector on a hard drive so that it is marked as bad and unusable to an OS, but sector actually is fine and holds malicious data.
Tempest	**Def** – study and control of spurious electrical signals that are emitted by electrical equipment. • Tempest equipment is implemented to prevent intruders from picking up info through the airwaves with listening devices. • Tempest is a standardized technology that suppresses signal emanations with shielding material. • The devices hav an outer metal coating referred to as a Faraday cage. • Expensive and 2 alternatives are **white noise** and **control zone concept.**
White Noise	**Def** – uniform spectrum of random electrical signals distributed over the full spectrum so that the bandwidth is constant and an intruder is not able to decipher real info from random noise or random info.
IDS	**Intrusion Detection Systems** – used to monitor a network or an individual computer **2 types** 1. **NIDS** – monitors a network or a segment of the network. • Used to uncover possible attacks or suspicious activities. 2. **HIDS** – monitors a particular system. • Usually used to make sure users do not accidentally delete system files, reconfigure important settings, or put the system at risk **2 Subsets of IDS** 1. **Knowledge or Signature-based IDS** 2. **Behavior-Based or Statistical IDS** – observes and detects deviation from expected behavior or users and systems • Can use **Expert System** technology which attempts to think like a human and provide reasoning. Can detect real-time anomalies and review audit log files to detect suspicious activity already taken place. • For an IDS to perform real-time anomaly detection it uses a **time-based induction Machine (TIM)**, which is a virtual machine that tracks and build behavior profiles for system use, network traffic, and user activities. • Can send an alert, kill the connection, or reconfig a router/FW to try and stop similar attacks **Network Traffic** – if network traffic volume exceeds IDS sensors threshold attacks can go unnoticed and each vendor has its own threshold. • In very high-network traffic environments , multiple sensors should be in place so that no

	packet can pass w/out being inspected. - Sensors can be set up to analyze each packet for different signatures.
5 Components of IDS	1. **Sensors** – Detects events and sends this data to the monitoring SW 2. **Central monitoring SW** – Accepts data from all sensors on the network and analyzes it 3. **Analysis of event reports** – Might offer a recommendation for counteracting the event. 4. **DB Components** – Determines if an IP address or an attack has been seen before (trend analysis). 5. **Response Boxes** – Take info from the previous components and respond to the event.
Honeypot	**Def** – a computer set up as a sacrificial lamb on the network and is not locked down. Used to entice an attacker to this computer instead of attacking authentic computers. **Delineation b/t enticement and entrapment:** 1. **Enticement** – system has open ports and services an attacker might want to take advantage of. 2. **Entrapment** – intruder is induced to commit a crime that they weren't originally contemplating. Its illegal.
Network Sniffer	**Def** – type of wiretap device that plugs into a network for the purpose of eavesdropping on network traffic. - Network traffic is in binary so the sniffer has a protocol analysis capability to recognize different protocols. - Very hard to detect and their activities cannot be audited.
Dictionary Attack	A program that is feed a dictionary of commonly used words and the program will hash the dictionary and compare to the message digest with the system password file that also stores its passwords in one way hash. **Countermeasures to password attacks:** - Do not allow psswds to be sent in cleartext - Encrypt the passwords with encryption algorithms or hashing functions - Employee one time password tokens - Use hard to guess psswds - Rotate passwords frequently - Employee IDS to detect behavior - Use dictionary attacks to find weak passwords chosen by users - Use complex psswds - Protect psswd files.
Brute Force Attack	Many types but overall it is an attack that continually tries different inputs to achieve a predefined goal. **Wardialing** – a brute force attack that dials a bunch of phone numbers looking for a modem. **Countermeasures:** - Perform brute force attacks to find holes - Make sure only necessary phone numbers are made public - Provide stringent access control methods that would make attacks less successful - Monitor and audit for such activity - Employ IDS - Set lockout thresholds.
Spoofing at Logon	A program that presents a fake logon screen can be presented by an attacker to trick the user to logon and thus gaining knowledge of credentials. **Countermeasures:** - Display # of failed logon attempts to the user - Use a **Trusted Path** – tells the user that he is communicating directly with OS (i.e. using ctrl+alt+del).
Penetration Testing	Simulating attacks on a network and the systems that make it up at the request of the owner. - Must have signed consent from the owner of the environment outlining what is to be accomplished in the test and what degree vulnerabilities should be tested. **5 Step Process:** 1. **Discovery** – Footprinting and gathering info about the target 2. **Enumeration** – Performing port scans and resource identification methods 3. **Vulnerability Mapping** – Identify vulnerabilities in identified systems and resources 4. **Exploitation** – Attempting to gain unauthorized access by exploiting vulnerabilities 5. **Report to mgmt –** Documentation of findings of test goes to mgmt along with suggested countermeasures **3 types of understanding the team can have before tests:** 1. **Zero knowledge –** Team has very minimal knowledge 2. **Partial Knowledge** – Team has some info about target. 3. **Full Knowledge** – Team has intimate knowledge of taret.

	• Team should start off with basic user level access

3. Security Models and Architecture

Topic	Description
Security Model	**Def** – a statement that outlines the requirements necessary to properly support and implement a certain security policy. • Provides a deeper explanation of how a computer OS should be developed to properly support a specific security policy. • Security is best if it is designed and built into the foundation of OS and applications and not added on as an afterthought. • Security that a product provides has to be rated on the availability, integrity, and confidentiality it provides.
Computer Architecture	Encompasses all the parts of a computer system necessary for it to function, including the OS, memory chips, circuits, hard drive, security components, buses, and networking components.
CPU	**Central Processing Unit** – a microprocessor that contains a control unit, an ALU, and registers. • All operations w/in the CPU are performed by electrical signals at different voltages in different combination, and each transistor holds this voltage, which represents 0s and 1s to the computer. • CPU contains registers that point to memory locations that contain the next instructions to be executed and enable the CPU to keep status info of the data that needs to be processed. Registers are not permanent storage areas but temporary memory area. • **ALU** – Arithmetic Logic Unit – Performs mathematical functions and logical operations on data. It's the brain of the CPU and the CPU is the brain of the computer. • **Control Unit** – manages and synchronizes the system while different applications code and OS instructions are being executed. • Determines what application instructions get processed and in what priority and time slice. • Controls when instructions are executed and this execution enable applications to process data. • Does not process the data it is the traffic cop telling traffic when to stop and start again. **Process** • SW holds its instructions and data in memory. When action needs to take place on the data, the instructions and data are passed to the CPU. • CPU components handle the flow of instructions from the OS and applications. • The data that needs to be process is passed into the instruction registers. When the control unit indicates that the CPU can process them they are passed to CPU for processing. • The results are sent back to the computer's memory so the application can use this processed data to continue its tasks. **Buffer Overflows** – Data processed by the CPU is done in blocks at a time. If the SW instructions do not properly set the boundaries for how much data can come in as a block, extra data can slip in. Problem with OS or application instructions. • If extra data slips in, it can be executed in a privileged mode and cause disruption and lead to unauthorized access or different degrees of damage.
Different types of Memory w/in a computer system	1. **RAM** – Random Access Memory – a type of memory storage facility where data can be held and altered. Used for read/write activities by the OS and applications. • Its volatile b/c if the computers power supply is terminated, then all info in this memory is lost. **2 Types of RAM** a. **Static** – Stores data without the need of being continually refreshed. b. **Dynamic** – requires that the data held be continuously refreshed b/c the data can dissipate and decay. 2. **ROM** – Read Only Memory – nonvolatile storage facility, meaning when a computer is turned off the data is still held w/in the memory chips. • When data is entered in ROM it cannot be altered. • SW stored in ROM is called Firmware 3. **EPROM** – Erasable and programmable read-only memory – can be modified, deleted, or upgraded. Holds data that can be electrically erased or written to. 4. **Cache Memory** – used for high-speed writing and reading activities. Holds instructions and

	data from primary storage and is accessed when application instructions and data are being executed. • Any info needed by the CPU very quickly, and very often, is often stored in cache.
Memory Mapping	B/c of different types of memory holding different info a computer system does not want to let every user, process, and application access all types of memory anytime and this is done using **memory mapping and addressing.** • CPU is most trusted component of a system and can access memory directly. CPU uses physical addresses instead of pointers to memory segments b/c CPU has physical wires connecting it to the memory chips w/in the computer. • B/c of physical connections b/t the two components physical addressing is used to represent the intersection b/t the wires and the transistors on a memory chip. • Software uses virtual or logical memory, using index tables and pointers, and accesses memory indirectly which is an access control layer b/t SW and memory. • When a program access memory, its access rights are verified and then instruction and commands are carried out in a way to ensure badly written code does not affect other programs. Applications and their processes can only access memory allocated to them. • If programs accessed data directly in memory, each program would have to wait until the prior program is done. **Secondary Storage** – nonvolatile storage media, which is a hard drive, floppy disks, or CD-ROM. **Virtual Storage** – the process of using RAM and secondary storage together. The system uses hard drive space to extend RAM memory space capability. • Hard drive space used to extend RAM is incremented in pages and when RAM memory is filled it will write data from memory onto the hard drive. • **Paging** – process of bringing data back from the hard drive to memory. Takes longer than info stored in memory. **4 Categories of memory** **1. Primary Storage** – Main memory directly accessed by the CPU and indirectly access by apps, considered volatile memory **2. Secondary Storage** – Nonvolatile storage (floppy, CD-ROM, hard drive, etc.) **3. Virtual Storage** – RAM and secondary storage used together. **4. RAM** – Where instructions and data are placed when being executed.
Protection Rings	**Def** – used as a protection mechanism to ensure process do not negatively affect each other or critical sys components, memory mapping is another mechanism. Provide strict boundaries and definitions for what the processes that work w/in each ring can access and what operations they can successfully execute. **Provide an intermediate layer b/t subjects and objects and used for access control when subjects try to access an object.** • Processes that operate w/in the inner rings have more privileges than the processes operating in the outer rings b/c the inner rings only permit the most trusted components and processes to operate w/in them. • Processes that execute w/in the inner rings are referred to as existing in a **privileged or supervisor role**. • Processes working in the outer rings are said to execute in a **user mode.** ***Actual ring architecture that is being used by a system is dictated by the processor and the OS. The processor is constructed to work w/ a certain number of rings and the OS must be developed to work with this structure. One reason why one OS will work with Intel, but not alpha chip.** • OS components operate in the inner rings to give them the most access to memory locations, peripheral devices, system drivers, and sensitive config and is most protected. Apps usually run in ring 3. • Commands and instructions sent to the CPU from Apps are restrictive in nature and if they fall outside of permissions level, the CPU treats as a violation and will attempt to shut down the app. **4 Protection Ring** • **Ring 0** – OS kernel • **Ring 1** – Remaining parts of the OS • **Ring 2** – I/O Drivers and Utilities • **Ring 3** – Applications and programs **Entities can only access objects w/in their own ring and outer rings.**
Process Activity	Some memory, data files, and variables are actually shared b/t different apps and is critical that more than one process does not attempt to read and write to these items at the same time. To prevent this the OS works with the CPU to provide time slicing and interrupts to ensure that processes are provided with adequate access to the CPU.

Process vs. Thread	**Process** – a program execution that works in its own address space and can only communicate with other processes in a controlled manner. **Thread** – represents a piece of code that is executed w/in a process. - Process can have one or more threads running at one time.
Operating Modes and States	**2 Operating Modes** 1. **Privileged (Supervisor State)** 2. **User Mode (Problem State)** **4 Operating States** 1. **Stopped** – Process is not running 2. **Waiting** – Process is waiting for an interrupt to be able to interact w/ the CPU 3. **Running** – Processes instructions are being executed by the CPU 4. **Ready** – Process is available to be used and waiting for an instruction. - When an app runs on a computer it thinks it is the only program running and does not know it is sharing resources. - **Virtual Machines** – created for apps to think they are the only ones running. Allotted a segmented of virtual memory.
Multi-threading, tasking, processing, and programming	**Multithreading** – A system that can process more than one request at a time. **Multitasking** – CPU process more than one process, or task, at one time **Multiprocessing** – A computer that has more than one processor (CPU) it can use them in parallel. **Multiprogramming** – Interleaved execution of 2 or more programs by a CPU.
Input/Output Device Mgmt	- OS uses a device driver to communicate to a device controller, which is an electrical component with its own SW used to provide a communication path enables a device and OS to exchange data. **Core responsibility of the OS.** - **Deadlock** – when resources (memory allocation, printer, disk space, etc.) are not released back into the pool of available resources for applications to use.
System Architecture	Security mechanisms can be placed at the HW, kernel, OS services or program layers. - At lower levels (HW) protection mechanisms are simple and broad. As ascend up the layers more complexity is added and functionality becomes more specific and granual. - Top Layer holds the most complexity b/c provides users functionality and options. - More complex security mechanisms becomes, less assurance it provides. - **For a mechanism to be trusted** it must protect itself and data its processing, performs in a predictable manner, and doesn't effect other trusted or untrused mechanisms adversely. In return trusted components have access to more privileged services.
TCB	**Trusted Computing Base** – total combination of protection mechanisms w/in a computer system (includes HW, SW, and firmware). - Originated from the Orange Book and address the level of trust not security. - Orange book defines a trusted system as HW and SW that utilize measures to protect the integrity of unclassified or classified data for a range of users w/out violating access rights and the security policy. - Each Layer of the system must trust the underlying layer.
Security Perimeter	**Def** – resources that fall w/in the TCB. Boundary that divides the trusted from untrusted. - For the system to stay in a secure state when a TCB component needs to communicate with a component outside of the TCB precise communication standards must be developed. Handled through interfaces. - **TCB and Security Perimeter are not physical entities, but conceptual constructs used by the OS to delineate b/t trusted and untrusted components.**
Reference Monitor and Security Kernel	Mechanisms that ensures that the subjects that access objects have been given the necessary permissions to do so. **Reference Monitor** – abstract machine (not a physical component) that mediates all access subjects have to objects to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification. - Subjects must be fully authorized prior to accessing an object. **Security Kernel** – Mechanisms that fall w/in the TCB and implements/enforces the reference monitor concept. Made up of HW, SW and firmware and is the **core of the TCB**. **4 Main Components:** 1. Provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. 2. Reference monitor must be invoked for every access attempt and must be impossible to circumvent.

	3. Reference monitor must be verifiable as being correct by all decisions being written to an audit log and verified as being correct. 4. Small enough to be tested and verified in a complete and comprehensive manner
Domains	**Def** – a set of objects that a subject is able to access. Defines which objects are available and not available to a subject. • Privileged and User modes are domains **Execution Domain** – a program residing in privileged domain being able to execute its instructions and process its data with the assurance that programs in a different domain cannot negatively affect its environment. • Security domain has a direct correlation to the protection ring. Lower the protection ring number the higher the privilege and larger the security domain.
Resource Isolation	Each resource has to be clearly separated from one another to properly enforce access control, auditing, and to determine what subjects and objects reside in specific domains. • Processes are isolated by using virtual memory • Systems of higher trust levels implement **hardware segmentation** of memory by segmenting physically.
Multilevel Security Policies	Security polices that prevent info from flowing from a high security level to a lower security level.
Least Privilege	**Def** – A process has no more privileges than necessary to be able to fulfill its functions.
Layering, Data Hiding, and Abstraction	**Layering** – Systems that meet trust levels must supply mechanisms that force processes to work in layers. Basic functionally takes place at lower layers and more complex, sensitive functions at higher layers. • Layers communicate but only through detailed interfaces that uphold security integrity of the system **Data Hiding** – Data in one layer is hidden b/c subjects in another layer do not know the data exists. **Abstraction** – Objects can be grouped into sets called classes. When a class of objects is assigned specific permissions and acceptable activities defined its called abstraction. • When a class is defined, all objects w/in the class are assigned an abstract data type, which is the precise definition of the format the object will accept data and the format it will present its processed data to other objects and subjects. • Provides a predictable communication and helps prevent authorized entities from modifying the data w/in an object inappropriately. *** methods to protect subjects, objects, and data w/in data.**
Relationship b/t a Security policy and Security Model	Security policy provides the abstract goals and the security model provides the dos and don’ts necessary to fulfill these goals
State Machine Models	**Def** – To verify the security of a system the state is used, which means all current permissions and all current instance of subjects access objects must be captured. • Maintaining the state of a system deals with subjects association with objects. • If subjects can only access objects by means that are concurrent with the security policy, the system is secure. • **Snapshot of a system in one moment of time** **State Transition** – Activities that can alter a state. • Systems that employ a state machine model will be in secure state in each and every instance of its existence. • Failing in a secure state is extremely important (system reboots, error messages, freezes)
Bell-Lapadula Model	A model that protects the **confidentiality** of the info w/in a system • Its a multilevel security system b/c users with different clearances use the systems and process data with different classifications. • **Information flow security model** – info does not flow in an insecure manner • Subject to object model by making sure subjects are properly authenticated, having necessary security clearance and need to know, to access an object. • **Uses security levels** **3 Rules/States the system can go into** 1. **Simple security rule** – A subject cannot read data at a higher security level (**no read up)** 2. ***-property rule** – A subject cannot write data to an object at a lower security level. **(no write down)** 3. **Strong star property rule** – A subject that has read and write capabilities can only perform those functions at the same level. **Problems with this model** 1. Addresses only confidentiality not integrity

	2. Does not address mgmt of access control, b/c there is no mechanism to modify access rights 3. Model does not prevent or address cover channels 4. Model does not address files sharing used in modern systems
Biba Model	A model that protects the **integrity** of the info w/in a system • **Information Flow Model** • Uses **Integrity levels** **2 Rules** **1. Simple Integrity axiom** – A subject cannot read data at a lower integrity level **(no read down)** • **This rule is protecting the subject and data at a higher integrity level from being corrupted by data in a lower integrity level.** **2. *-integrity axiom** – A subject cannot modify an object in a higher integrity level **(no write up)** **Tip to remember: If simple is used it is talking about reading, if * or star is used its talking about writing.** **Of the three main goals of integrity Biba only address** "Prevent unauthorized users from making modifications."
Clark-Wilson Model	An integrity model implemented to protect the integrity of data and to ensure that properly formatted transactions take place. • Focus on preventing authorized users from making unauthorized modification of data, or commit fraud and errors w/in commercial applications. • **Subjects can only access objects through authorized programs** (Access triple – subject-application-object). • Separation of duties is enforced by dividing an operation into different parts and requiring different users or rules to perform each part. • Auditing is required. **Goal of Integrity – Clark-Wilson address all three** 1. Prevent unauthorized users from making modifications 2. Prevent authorized users from making improper modifications 3. Maintain internal and external consistency
Information Flow model	Information is restricted in its flow to only go to and from entities in a way that does negate the security policy.
Noninterference Model	Commands and activities performed at one security level should not be seen or affect subjects or objects at a different security level • Actions at a higher security level do not affect or interfere with actions at lower levels. • If a lower level entity was aware of certain activity that took place by an entity at a higher level and the state of system changed for this lower level, the entity might be able to deduce info of higher state, which is a way of info leakage.
Brewer and Nash model	**Chinese Wall Model** - Access controls change dynamically depending on a users previous actions to protect against data that may be seen as conflicts of interest.
Graham-Denning model	Creates rights for subjects, which correlate to the operations that can be executed on objects.
Harrison-Ruzzo-Ullman model	Allows for access rights to be changed and specifies how subjects and objects should be created and deleted.
4 Security Modes of Operation	**1. Dedicated Security Mode** – system is operating in dedicated security mode if all users have the clearance and formal **need to know** to all data processed within the system • Users have access to all data and have a need to know • Have signed a nondisclosure agreements. • Handles a single classification level of info **2. System-High Security Mode** – System is operating in system-high security mode when all users have a security clearance or authorization to access the info **but not necessarily the need to know** for all info process on the system. • Users only have a need to know for some data. • This mode requires all users to have the highest level of clearance required by any and all data on the system **3. Compartmented Security Mode** – A system is operating in compartmented security mode when users have the clearance to access all info, but do not have the need to know and formal access approval. • Users are restricted from being able to access some info b/c they do not need it to perform job functions.

	• Users can access a segment or compartment of data only • **Compartmented mode workstations (CMWs)** – enable users to process multiple compartments of data at the same time, if they have the necessary clearance. **5. Multilevel Security Mode** – handles multiple info classifications at a number of different security levels w/in one system (Bell-LaPadula model)
Trust and Assurance systems	**Trusted systems** – all protection mechanisms work together to process sensitive data for may types of uses and still maintains the same secure state **Assurance in systems** – their designs were thoroughly inspected, the development states were review, the technical specifications and test plans evaluated, and the system was extensively tested.
Orange Book	US dept of defense developed and it is called **Trusted Computer System Evaluation Criteria (TCSEC)** – used to evaluate OS, applications, and different products **For the military**. • Deals with stand-alone systems • **Addresses only confidentiality and security** • Security mechanisms and assurance of those mechanisms are not evaluated separately, but combined and rated as a whole. • Compared to **Bell-LaPuda Model** **Graded Levels of Classification** **A** – Verified protected **B** – Mandatory Protection (Security Labels) **C** – Discretionary protection **D** – Minimal Security
D1	System provides minimal security and is used for systems that were evaluated but failed to meet the criteria of higher divisions
C1 & C2	**C1** – outlines access control to be based on individuals/or groups. Requires separation of duties, and identification and authentication of individual entities. • Users are processing info at the same sensitivity level • Supply a protected execution domain so privileged system processes are not adversely affected by lower privileged processes. **C2** – Same as C1 but requires object reuse protection and auditing. • Most reasonable for commercial applications
B1, B2, B3	**B1** – Labeled Security – First rating that requires security labels (classification & clearance labels) • Intended for systems that handle classified data. **B2** – Structured Protection – Requires all subjects and devices to have security labels, there must be a trusted path and covert channel analysis, and separate admin functionality is provided from operations. • Distinct address space provided to isolate processes • Security policy is clearly defined and documented • Used in systems that process sensitive data. **B3** – Security Domains – A Security admin role is defined trusted recovery takes place, and system monitors events and notifies security personnel. • Design and implementation should not provided too much complexity • Reference monitor small enough to test and be tamperproof • Processes very sensitive info
A1	**A1** – Verified design – Difference from B3 is the way that the system was designed and developed is evaluated in a much more structured and stringent procedure. • Processes Top Secret Info
Rainbow Series	Books written to cover many other topics in security that are not addressed by Orange book.
Red Book	**TNI** – Trusted network interpretation – AKA Red Book – Addresses security topics for networks and network components (LAN/WAN). • Rates confidentiality and integrity of data **Ratings:** **None** **C1** – Minimum **C2** – Fair **B2** – Good
ITSEC	**Information Technology Security Evaluation Criteria** – First attempt at est. a single standard for evaluating security attributes of computer systems by many European Countries. • 2 Main attributes of evaluating a system: **Functionality and Assurance.** • Assurance is the degree of confidence in a security components and its effectiveness. Tested by examining development practices, documentation, config mgmt, and testing mechanisms.

	• ITSEC rates the 2 attributes, functionality and assurance, separately – TCSEC evaluate attributes together. • E0 – E6 rate assurance and F1 – F10 rate functionality
Common Criteria	ISO commission to create and a number of national security standards organizations worked to create. • Helps manufactures b/c they can build to one specific set of requirements • Provides more flexibility by evaluating a product against a **protection profile**. • Assess based on the threats being faced today. • **EAL** – Evaluation Assurance Level – What the criteria assigns to a product • Each threat is listed along with how it is to be controlled by specific objectives • Assess **Functionality and Assurance** **Components of Common Criteria:** • **Protection Profile** – Description of needed security solution. • **Target of evaluation** – Product proposed to provide needed security solution • **Security Target** – Written by vendor explaining security functionality and assurance mechanisms that meet the needed security solution. What the product does and how it does it. • **Packages – EALs** – Functional and assurance requirements are bundled into packages for reuse. Component describes what must be met to achieve specific EAL ratings
Certification vs. Accreditation	**Certification** –Technical evaluation of the security components and their purpose of accreditation. Assess the security mechanisms and controls and evaluates effectiveness. **Accreditation** – Mgmts official acceptance of the information in the certification process. Mgmt understands level of protection the system will provide and understands security risks. ***Because SW, systems, and environments continually change the certification and accreditation should continually take place**
7799 Standards	**British 7799 Standards or ISO 17799 (Code of practice for Info Security Mgmt)** – Risk based method for assess, evaluating, and managing risks. • Approach to addressing security as a whole, not just technical. • Creates a security program
Open vs. Closed systems	**Open systems** – Built upon standards, protocols, and interfaces that have published specifications, which enable third-party vendors to develop add-on components and devices **Closed Systems** – Use an architecture that does not follow industry standards. Are proprietary meaning they will only communicate with like systems
Cover Channels	**Def** – a way for an entity to receive info in an unauthorized manner. It is an info flow that is not controlled by a security mechanism or the mechanism has been successfully compromised. • This info path is usually not used for communication, thus the system does not properly protect. • Violates security policy of the system **2 types:** 1. **Covert timing channel** – One process relays info to another by modulating its use of system resources, which can be accessing the hard drive, using excessive CPU cycles or head placement on a drive track. 2. **Covert Storage Channel** – when a process writes data to a storage location and another process directly, or indirectly reads it **Loki attack** – A cover channel attach that uses ICMP protocol by an attacker writing data right behind the ICMP header. **Countermeasures:** • Hard to detect and all systems have some form of covet channel • IDS may detect, probably not • HIDS usually more successful of finding • Auditing should be enabled to try and detect a covert channel use pattern.
Backdoors	**AKA Maintenance Hooks** – Are instructions w/in the SW that only the developer knows and can invoke and are placed for easy access bypassing security controls. **Countermeasures:** • Code reviews, unit and integration testing looking for backdoors. • HDS • File permissions can be set to protect sensitive info from modification. • Strict access control can be enforced in the first place • File system encryption • Auditing enabled to detect.
Asynchronous Attack	**Def** – Takes advantage of the way a system process requests and performs tasks. Deals with the

	sequences of steps a system uses to complete a task. **TOC/TOU** – Time of check vs. time of use – Using a timing difference when the system checks to see if a file exists and when its executed. File can be modified during than space of time. **Race Condition** – manipulating the way a process is supposed to work and changing the sequence. I.e. process 1 goes first and process 2 goes second. Process modified for process 2 to perform first. **Countermeasure:** • HIDS • File system permissions and encryption • Strict access control measures • Auditing enabled
Buffer Overflows	**Def** – happen when programs do not check the length of data that is inputted into a program and allow more data than is allotted by memory and executed by the CPU. • **AKA Smashing the Stack** • Usually aimed at systems that allow the extra code be executed with privileged rights. **Countermeasures:** • Proper programming and good coding practices • Tools that monitor DLL usage and tools that provide a wrapper around the kernael to watch for known buffer overflow attacks. • HIDS • File system permissions and encryption • Strict access control measures • Auditing enabled

4. Physical Security

Topic	Description
Physical Security	• The first line of defense against environmental risks and unpredictable human behavior. • Implemented in a layered defense model with controls working together in a tiered architecture.
EAC Tokens	Electronic Access Control tokens – used in physical security to authenticate subjects. Can be proximity readers, programmable locks, or biometric systems.
Planning Process for setting up Physical Sec	First the value of property w/in the facility and the value of the facility itself need to be ascertained to determine the proper budget for physical security so that controls can be cost effective. • Value can be determined by doing a critical path analysis. • Critical path analysis lists all pieces of an environment and how they interact and are interdependent. **The pat for critical business functionality.** • **Redundant paths should be in use for every critical path.**
Looking for facility locations	Consider crime, natural disaster possibilities, and distance to hospitals, police/fire stations, airports, and railroads. • Behind hills limits electrical transmissions • No or very little signage.
Construction	Physical construction material and structure composition need to be evaluated for their protective characteristics (fire protection which is fire rating), utility, and costs/benefits. • **Load** of a building's walls, floors, and ceilings need to be estimated and projected to ensure that the building will not collapse. **Major Items that need to be addressed:** 1. **Walls** • Combustibility of material • Fire rating • Reinforcements for secured areas 2. **Doors** • Combustibility of material • Fire rating • Resistance to forcible entry • Emergency marking • Placement • Alarms • Type of glass – shatterproof or bulletproof • Electronic door locks that revert to a disable state for safe Evac in power outages.

	3. **Ceilings** • Combustibility of material • Fire rating • Load bearing weight • Drop Ceiling considerations 4. **Windows** • Translucent or opaque • Shatterproof • Alarms placement accessibility to intruders 5. **Flooring** • Load and weight rating • Combustibility of material • Fire rating • Raised flooring • Nonconducting surface and material 6. **Heating, ventilation, and air conditioning** • Positive air pressure • Protected intake vents • Dedicated power lines • Emergency shutoff valves and switches • Placement 7. **Electrical power supplies** • Backup and Alt power supplies • Clean and steady power source • Dedicated feeders to required areas • Placement and access to distribution panels and circuit breakers 8. **Water and Gas Lines** • Shutoff valves • Positive flow (material flows out of building, not in) • Placement 9. **Fire detection and suppression** • Placement of sensors and detectors • Placement of sprinklers • Type of detectors and sprinklers.
Facility Components	**Internal Partitions** – used to create barriers b/t one area and another. • Surfaces that conduct electricity should be avoided in sensitive electrical areas • Data centers should not be located on the top floors, in case of a fire, or in the basement b/c of flooding. Should be in the core of the facility.
Threats that physical security combats	• Theft • Interruptions to services • Physical Damage • Compromised system integrity • Unauthorized disclosure of info
Physical Security component selection process	A security mechanisms should be cost beneficial – means that the reduction in potential loss is significantly greater than the cost of implementing the mechanism in the first place and the cost of lifetime maintenance.
Hardware	**SLA** – Service level Agreements – Used for hardware maintenance **MTBF** – Mean Time B/t Failure – estimates the expected lifetime of a device or element w/in a device. **MTTR** – Mean Time to Repair – estimates the time it will take to repair the device and get it back into production.
Power protection	**3 main methods of protecting against power problems:** 1. **UPS** – uses batteries that range in size and capacity that provide extra power. **Two types of UPS** a. **Online systems** – Use AC line voltage to charge a bank of batteries. When in use the UPS has an inverter that changes the DC output from the batteries into the required AC form and regulates the voltage as it powers computer devices. b. **Standby UPS** – Stays inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery bank. 2. **Power line conditioners**

	3. **Backup sources**
Electrical Power Issues	**2 types of power sources**: 1. **Primary power source** – used for day-to-day operations. Has at least 1 dedicated feeder from a utility station or power grid. 2. **Alternate power source** – Used in the event of a failure of the primary power source. Take the form of UPS, Generator, or batteries **Electrical Power Definitions:** a. **Ground** – The pathway to the earth to enable excessive voltage to dissipate b. **Noise** – Electromagnetic or frequency interface that disrupts the power flow and can cause fluctuations c. **Transient Noise –** Short duration of power line disruption d. **Inrush current** – The initial surge of current required when there is an increase in power demand e. **Clean Power** – Power that does not fluctuate. When clean power is being used it means that the power supply contains no interferences or voltage fluctuations. **Types of Interference or line noise –** 1. **EMI** – Electromagnetic interface – Created by the difference b/t 3 wires: Hot, neutral, and ground. Lightning and electrical motors can induce EMI. 2. **RFI** – Radio Frequency Interface – Created by the components of an electrical system such as electrical cables and fluorescent lighting.
Types of voltage fluctuations	1. **Power Excess** • **Spike** – Momentary high voltage • **Surge** – Prolonged high voltage – protected by surge protectors 2. **Power loss** • **Fault** – Momentary power out • **Blackout** – Prolonged loss of power – voltage drops to zero 3. **Power degradation** • **Sag/Dip** – Momentary low voltage • **Brownout** – Prolonged power supply that is below normal voltage
Noise	On a power line takes place when electrical interference is superimposed onto the power line. **Voltage regulators and line conditioners** – used to ensure a clean and smooth distribution of power
Power Preventive measures and good practices	• Shut down devices in an orderly fashion • Do not have devices or media around powerful magnetic lines, energized conductors, or circuits that could create magnetic fields • Use shielded lines to protect form magnetic induction • Shield long cable runs • Use 3 prong connection and adapters if using 2 prong cables
Personnel Controls that effect physical security	1. **Pre-employment Screening** • Check references – employment/education • Character eval • Background/drug check 2. **Employee Maintenance** • Periodic reviews • Reeval security clearances • Supervisor updates and recommendations • Job rotation • Separation of duties 3. **Post-employment** • Friendly termination • Exit interview • Escorting from facility • Locking and removing computer accounts • Recover company property
Environmental Issues	Maintain appropriate temperature/humidity • High humidity can cause corrosions and low humidity can cause excessive static electricity • Humidity of 45 – 60 percent is acceptable for areas processing data • Low temps can cause mechanisms to slow down/stop and high temps cause devices to use too much fan power and eventually shut down

<table>
<tr><td></td><td>• Temp for computing devices should fall into 70 – 74 degrees
• <b>Hygrometer</b> – monitors humidity
<b>Damaging temperatures</b>
Computer sys and peripherals – 175 F
Magnetic media – 100 F
Paper products – 350 F</td></tr>
<tr><td><b>Ventilation</b></td><td>A closed loop recirculating air-conditioning system should be installed to maintain air quality. Closed loop means that the air w/in the building is reused after filtration
<b>Positive Pressure</b> – When a door is open air goes out and outside air does not come in. For air quality and to get smoke to go out when there is a fire</td></tr>
<tr><td><b>Fire prevention, detection and suppression</b></td><td><b>Fire Prevention</b> – training employees how to react properly to a fire, supplying the right equipment and ensuring that it is in working order.
<b>Fire Detection</b> – automatic sensors.
<b>Fire Protection –</b> early smoke detection and shutting down systems.</td></tr>
<tr><td><b>Types of fire detection</b></td><td><b>Located on the ceiling, installed below raised floors and located in enclosures/air ducts</b>

<b>Smoke Activated</b> – good for early warning devices and can be used to sound a warning alarm before sprinklers turn on.
• <b>Photoelectric device</b> – AKA optical detector – Produces a beam o light across a protected area and if the bean is obstructed the alarm assumes its smoke and sounds.
• Another type of photoelectric device samples the air by drawing air into a pipe.
<b>Heat Activated</b> – can either alarm when a predefined temperature is reached or can detect an increase in temperature that exceeds a predefined rate or a combo of both.
• <b>Rate of Rise temp sensors</b> usually provide quicker warning, but cause more false alarms than <b>fixed temp sensors.</b></td></tr>
<tr><td><b>Flame Activated</b></td><td>Either senses the pulsations of a flame or senses the infrared energy that is associated with flames and combustion
• Usually more expensive than other detectors
• Usually used in special cases w/ high valued equipment
• Respond more quickly, releasing an agent, and sound an alarm.</td></tr>
<tr><td><b>Automatic dial-up alarm</b></td><td>Configured to call the local fire station/police to report a detected fire. Plays a prerecorded message
• Usually combined with one of the previous detection methods.</td></tr>
<tr><td><b>Plenum Area</b></td><td>Where wiring and cable are strung through. Drop down ceilings, in the walls, and under raised floors.
<b>Plenum rated cabling</b> should be used b/c it is made out of material that does not let off hazardous gases if it burns.</td></tr>
<tr><td><b>Fire suppression</b></td><td>• Suppression agents should be located in different areas
• Agents have a zone of coverage
• If an agent uses CO2 should have a delay mechanism and an alarm to alone people to get out. Best used in unattended facilities.
• Halon, used in small amounts will not affect people, but depletes the ozone. Banned in 92
• FM-200 is similar to halon, but does not destroy the ozone.
• HVAC (heating, ventilation, air-conditioning) is a fire suppression issue. Should be connected to the alarm system and shut down when there is a fire to supply as little air as possible.</td></tr>
<tr><td><b>4 types of fire and suppression methods</b></td><td><table>
<tr><th>Fire Class</th><th>Types of Fire</th><th>Elements of fire</th><th>Suppression Method</th></tr>
<tr><td>A</td><td>Common Combustibles</td><td>Wood products, paper, and laminates</td><td>Water or soda acid</td></tr>
<tr><td>B</td><td>Liquid</td><td>Petroleum Products</td><td>Gas (halon), CO2, or soda Acid</td></tr>
<tr><td>C</td><td>Electrical</td><td>Electrical equipment and wires</td><td>Gas (halon) or CO2</td></tr>
<tr><td>D</td><td>Combustible Metals</td><td>Magnesium, sodium, potassium</td><td>Dry Powder</td></tr>
</table></td></tr>
<tr><td><b>How different substances interfere w/ elements of fire</b></td><td><table>
<tr><th>Combustion Elements</th><th>Suppression Methods</th><th>How Suppression works</th></tr>
<tr><td>Fuel</td><td>Soda Acid</td><td>Removes fuel</td></tr>
<tr><td>Oxygen</td><td>CO2</td><td>Removes oxygen</td></tr>
<tr><td>Temperature</td><td>Water</td><td>Reduces temperature</td></tr>
<tr><td>Chemical Combustion</td><td>Gas – halon or halon substitute</td><td>Interfaces w/ the chemical reactions b/t elements</td></tr>
</table></td></tr>
<tr><td><b>Water Sprinklers</b></td><td>Sensors should be used to shut down electrical power before water sprinklers activate. Each sprinkler head should activate individually to avoid wide-area damage, and there should be shutoff valves.
<b>4 main types of sprinkler systems:</b>
1. <b>Wet pipe – AKA Close Head System –</b> always contains water in the pipes and are usually discharged by temperature control level sensors.
• Disadvantage is pipe may freeze and break</td></tr>
</table>

	• Sprinkler heads are closed until activation. **2. Dry Pipe** – held back by a valve until a specific temperature is reached. • Delay can be a good thing because it provides time for some one to shut down the system in a false alarm • Best used in colder climates b/c pipes will not freeze. **3. Preaction** – a combo of wet and dry pipe systems. Water is not held in the pipes and is only released into the pipes once a predefined temp is reached. Once the pipes are filled with water it does not release until a link is melted and then water is disbursed. • Usually chosen for equipment that is costly and prevent water damage. **4. Deluge** – same as a dry pipe system but the sprinkler head is open. Large amounts of water are disbursed. • Not used in data processing environments.
Emergency Response and Procedures	• Evacuation procedures • System shutdown • Training and drills • Integration with DR plans • Easily accessible documented procedures for different types of emergencies • Periodic equipment tests
Perimeter security	First line of defense. **Works in 2 modes** 1. Security practices during operation 2. Security during the time the facility is closed • Deals with access control, surveillance monitoring, intrusion detection, and corrective actions.
Facility Access Control	• Objectives of physical access controls and the protection of people's lives may come into conflict. In these situations, **a persons life always takes precedence**. • Access control points will be identified and classified as external, main, and secondary entrances.
Locks	Locks and keys are the most inexpensive access control mechanism. • Locks are considered deterrents to semi-serious intruders and delaying devices to serious intruders. • Part of the protection scheme, but not the sole. **Types** **1. Preset Locks** – These locks are usually used on doors. Can be a key and knob combination, mortise, or rim locks with latches and deadbolts. **2. Cipher Locks** – AKA programmable locks – use keypads to control access into an area or facility. • Should have a visibility shield to stop shoulder surfing **Options on cipher locks that improve performance:** • **Door Delay** – if a door is held open for a given time an alarm will trigger. • **Key Override** – A specific combo can be programmed for use in emergency situations. • **Master Keying** – Enables supervisory personnel to change access codes and other features of the cipher lock. • **Hostage Alarms** – A special code that can be used when an individual is under duress that can communicate to guard or police • **Device Locks** – Cable locks on devices.
Types of device locks	**Switch Controls** – covers on/off power switches. **Slot locks** – a bracket is mounted in a spare expansion slot, and a steel cable is used to secure the system to a stationary component. **Port Controls** – Blocks access to disk drives or unused serial/parallel ports. **Peripheral switch controls** – Secure a keyboard by inserting an on/off switch b/t the system unit and the keyboard input slot. **Cable traps** – Prevent the removal of input/output devices by passing cables through a lockable unit.
Piggybacking	Individual follows another person closely through a door w/out providing credentials
Card badge reader types	**1. Magnetic Cards** – cards that have embedded magnetic strips that contain access info. • If card is a memory card then the reader will pull info from it and make an access decision • If card is a smart card the individual may be required to enter a pin or password, which the card reader compares against the info on the card

	2. **Wireless proximity readers** – Two types are user activated and system sensing a. **User activated** – user swipes a card through the reader b. **System sensing** – will recognize the presence of an approaching object w/in a specific area. Reader sends the credentials to an authentication server which makes the access decision.
3 types of system sensing cards	1. **Transponders** – card and reader have a receiver, transmitter and battery. Reader sends signals to the card to request info and the card sends the reader an access code. 2. **Passive Devices** – card does not have a power source, but uses power from the reader. 3. **Field powered devices** – Card and reader contain a transmitter and active electronics. Card has its own power supply.
Fencing	• Works as a preventive and deterrent mechanism • Provide crowd control and access to entrances and facilities • Can be costly and unsightly **Heights of fences and security** a. 3 – 4 ft high only deter casual trespassers b. 6 – 7 ft high are considered too high to climb easily c. 8 ft high with strands of barbed wire at top are serious about protecting property. Will deter the more determined intruder. • Critical areas should have fences of at least 8ft high. • Bollards are small concrete pillars outside a building and deter someone from driving a car into the building • PIDAS fencing – Perimeter Intrusion Detection and Assessment Systems – fencing that has sensors on the wire mesh at the base of the fence.
Lighting	Used to discourage intruders and proived safety for personnel, entrances, parking areas, and critical sections. • Provides preventive and deterrent protection • NIST standard to protect critical areas is lighting should be 8 ft high and use 2 ft candles • Types of lighting – search lights, floodlights, and fresnel units (contain small lenses that can be focused)
3 types of Surveillance devices	1. **Patrol force/guards** – one of the best security mechanisms • More flexible than other security measures, provides good response, and is a great deterrent. • Is costly • Screening and bonding is important 2. **Dogs** 3. **Visual Recording devices** – works in conjunction with guards • **Closed Circuit TVs (CCTVs)** – enables a guard to monitor many different areas at once from a centralized location. **Should be coupled with other alert devices.**
5 types of Detecting devices	Detecting devices are used to sense changes that take place in an environment. 1. **Proximity Detection System** – AKA capacitance detector emits a measurable magnetic field and if the field is disrupted an alarm sounds. • Used to protect specific objects not a whole area/room. 2. **Photoelectric or Photometric System** – detects the change in the level of light w/in an area. • Must be in a windowless room • Work like photoelectric smoke detectors that emit a beam of light that is expected to hit the receive. If the beam is disrupted an alarm sounds 3. **Wave Pattern** – Generate a wave pattern that is sent over an area and reflected back to a receiver and if the patterns are returned altered an alarm sounds. 4. **Passive Infrared System** – Identifies the changes of heat waves in an area. If the particle temp w/in the air rise could be an intruder. 5. **Acoustical Seismic Detection System** – Detects the changes in noise level/vibration in an area. • Considered passive devices • Size and shape of a room and the items w/in a room may cause barriers. • More detectors needed to provide the necessary level of coverage.
Intrusion Detection systems or burglar alarms	• Most popular types use types that detect a change or break in a circuit such as foil embedded or connected to windows • Vibration detectors can detect movement on walls, ceilings, and floors when the fine wires embedded w/in the structure are broken
Doorways	Mantraps and turnstiles used so that unauthorized individuals entering a facility cannot get out if activated • Some mantraps use biometric systems that weigh a person who enters.

	- Doorways with automatic locks can be configured to be fail-secure or fail-safe. - **Fail secure** – door would default to being locked if power failed - **Fail-Safe** – in a power disruption

5. Telecom and Network Security

Topic	Description
OSI	**Open Systems Interconnect** – Worldwide federation that works to provide international standards
Protocol	A standard set of rules that determine how systems will communicate across networks
Application Layer	**Layer 7** – works closest to the user and does not include the actual applications, but the protocols to support the applications. **Protocols that work at this layer:** - SMTP - HTTP - LPD (line printer daemon) - FTP/TFTP - telnet Applications communicate with underlying protocols through APIs **Encapsulation: User Data**
Presentation Layer	**Layer 6** – formats the data into a standardized format and deals with the syntax of the data, not the meaning. Translates the format an application is using to a standard form used for passing messages over a network. **Protocols that work at this layer:** - TIFF - JPEG - GIF **Layer also handles data compression and encryption** **Encapsulation: User Data**
Session layer	**Layer 5** – Sets up, maintains, and breaks down the dialog (session) b/t 2 applications. Controls session organization and synchronization. - Provides session restart and recovery and maintenance of the session AKA **Session Mgmt** **Protocols that work at this layer:** - NFS - SQL - RPC **3 different modes of communication at this layer:** - **Simplex** – Communication takes place in one direction - **Half-duplex** – Communication takes place in both directions, but only one application can send info at a time. - **Full-duplex** – Communication takes place in both directions, and both apps can send info at the same time. **Encapsulation: User Data**
Transport layer	**Layer 4** – Deals w/ error detection and correction, regulates the flow of traffic, and multiplexes data. Provides end-to-end connectivity, sequencing, and virtual circuits. - Session layer is setting up communication b/t the applications and the transport layer is setting up communication b/t the computer systems. **Protocols that work at this layer:** - TCP - UDP - SPX - SSL **Encapsulation: Segment**
Network Layer	**Layer 3** – Provides routing, segmenting and relaying of data. Can determine alternate routes to avoid network congestion. - Inserts info into the packets header for proper routing **Protocols that work at this layer:** - IP - IPX - ICMP

	• RIP • BGP • OSPF • IGMP – Internet group mgmt protocol **Encapsulation: Packet**
Datalink Layer	**Layer 2** – Prepares data for the network wire by framing it. Where different LAN/WAN technologies live • Combination of bits into bytes and bytes into frames • Responsible for locating hosts on an internetwork • Access to the media using MAC address • MAC sublayer provides error detection; LLC sublayer provides error correction. • Format the frame for transmission over token ring, Ethernet, ATM, and FDDI networks. • Specifies the proper bit patterns for each technology of the network. **Protocols that work at this layer:** • SLIP • PPP • RARP • L2F • L2TP • FDDI • ISDN • ARP **Encapsulation: Frame**
Physical layer	**Layer 1** – Provides physical connections for transmission and performs electrical encoding of data. Transforms bits to electrical signals. • Translates info into electrical encoding and electrical state transitions **Protocols that work at this layer:** • HSSI – High speed serial interface • X.21 • EIA/TIA – 232 and EIA/TIA – 449 • Ethernet **Encapsulation: Bits**
TCP/IP	Suite of protocols that govern the way that data travels from one device to another. **Socket** – When TCP or UDP message and formed a source and destination port are contained w/in the header info along with the source and destination address. **TCP Handshake** 1. Host initiates a communication and sends a SYN packet to receiver 2. Receiver acknowledges by sending a SYN/ACK packet 3. Sending host acknowledges with an ACK packet 4. Session is now set up and is considered full duplex
Ports	**23 – Telnet** **25 – SMTP** **20 & 21 – FTP** **80 – HTTP** **161 & 162 – SNMP**
IPv4 vs. IPv6	**IPv4** – uses 32 bit for its address **IPv6 –** uses 128 bits for address, thus has more addresses to work with than IPv4.
Analog and digital signals	**Analog signals** – are continuously varying electromagnetic waves that can be carried over air, water, twisted pair, coaxial, or fiber optic. • Through a process of **Modulation** data is combined w/a carrier signal of a specific frequency. • The modulation of a signal differs in **Amplitude** (Height of the signal) and **Frequency** (number of waves in a defined period of time) • Only communication that is still analog is copper wiring that goes from a residential house or business to telephone companies CO called a local loop. **Digital signals** – Represent binary digits as electrical pulses with each pulse representing a 0 or 1. • Computer use for communication and when connected to a phone line use a Modem to transform the digital signal to analog. • Bandwidth refers to the number of electrical pulses that can be transmitted over a link w/in a second • More reliable over a longer distance than analog • Can transport more calls and data transmissions on the same at higher quality
Asynchronous and	**Asynchronous** – used when 2 devices are not synchronized in any way. The sender can send data at any

Synchronous communication

time and the receiving end must always be ready. Transfers data sequentially, uses start and stop bits, and requires that communicating devices communicate at the same speed

- Used to transmit small amounts of data
- Example is a terminal and a terminal server
- Modems use

Synchronous – Takes place b/t 2 devices that are synchronized, usually via a clocking mechanism

- Used to transmit large amount of data.
- Transfers data as a stream of bits
- Synchronization can happen b/t 2 systems using the same clocking mechanism, or a signal can be encoded into the data stream to let the receiver synchronize with the sender of the message.

Broadband and Baseband

Baseband – transmission method that is accomplished by applying direct current to a cable.

- Uses the entire cable for transmission
- Only allows one signal to be transmitted at a time.
- Ethernet is a baseband technology that uses the entire line for communication

Broadband – divides the cable into channels so that different types of data can be transmitted at the same time.

- Provides transmissions higher than 56kbps
- Examples: Leased line (T1, T3), ISDN, ATM, DSL, broadband wireless, and CATV.

Network Topologies

Topology	Characteristics	Problems	Tech that usually work
Bus	Uses a liner, single cable for all computers attached. All traffic travels the full cable and can be viewed by all other computers	One station experiences a problem, can negatively affect surrounding computers on same cable	Ethernet
Ring	All computers are connected by a unidirectional transmission link and the cable is in a closed loop	One station experiences a problem, can negatively affect surrounding computers on same ring.	FDDI
Star	All computers are connected to a central device, which provides more resilience for the network	Central point is a single point of failure.	Logical Bus (Ethernet) and ring technologies
Tree	Bus topology that does not have one linear cable, but instead uses branches of cables		Ethernet
Mesh	Computers are connected to each other, which provides redundancy	Requires more expense in cabling and extra effort to track down cable faults	Internet

LAN vs. WAN

What defines a LAN compared to a WAN depends on what takes place at the D-link layer.

When does a LAN become a WAN?

- If two LANs are connected by a different D-link layer technology, such as frame relay or X.25 we are looking at a WAN.

Ethernet

- Defined by the IEEE 802.3 standard
- Shares media (all devices take turns using the same media and detect collisions)
- Use broadcast and collision domains.
- Use CSMA (Carrier Sense Multiple Access) access method
- Supports full-duplex on twisted pair implementations
- Can use coaxial or twisted pair media
- 10mbps – 1gbps

Different Types of Ethernet

Ethernet Type	Cabling Type	Speed
10base2, ThinNet	Coaxial	10 Mbps
10base5, ThickNet	Coaxial	10 Mbps
10base-T	UTP	10 Mbps
100base-TX, Fast Ethernet	UTP	100 Mbps
1000base-T, Gigabit Ethernet	UTP	1000 Mbps

Token Ring

Token passing technology with a star configured topology.

	• Each computer is connected to a central hub called a **MAU** – Multistation Access Unit • **Active Monitor** – Removes frames that are continually circulating on the network. Occur if a computer locks up or taken offline and cannot receive a token destined to it. • **Beaconing** – If a computer detects a problem with the network, it sends a beacon frame. The frame generates a failure domain, which is b/t the computer that issued the beacon and its neighbor downstream. The computers and devices w/in the failure domain will attempt to reconfigure certain settings to try and work around the detected fault. • 4 – 16 Mbps
FDDI	**Fiber Distributed Data Interface** – Developed by ANSI (American National Standards Institute), is a high-speed token passing media access technology. • Speed of 100 mbps • Used as a network backbone using fiber optic cabling • Fault tolerance is provides by dual counter rotating rings • Used for distance up to 100 Kilometers and often used in MANs. • Version of FDDI, CDDI (Copper Distributed Data Interface), works over UTP and used in a LAN environment.
Cabling	**Bandwidth** – indicates the highest frequency range that it uses. Size of the pipe **Data Rate** – Actual data throughput of a cable after compression and encoding have been used. Amt of data that can be transferred through the pipe. **Types:** 1. **Coaxial** • Can work in baseband or broadband • More resistant to EMI, provides higher bandwidth, and longer cable lengths when compared to twisted pair. 2. **Twisted-Pair** • **STP** – Shielded twisted pair – cable has an outer foil shielding that protects from radio frequency inteference. • **UTP** – Unshielded twisted pair – does not have the foil shielding 3. **Fiber-Optic** – uses a type of glass that carries light waves. • Higher transmission speeds over longer distances • Not affected by attenuation and EMI • Usually used in backbone networks and environments that require high data transfer rates.
3 Cabling Problems	1. **Noise** – caused by surrounding devices or characteristics of the wirings environment 2. **Attenuation** – loss of signal strength as it travels. The effects of attenuation increase with higher frequencies. 3. **Crosstalk** – when electrical signals of one wire spill over to another wire. • UTP is susceptible and causes integrity degradation and data corruption.
Pressurized Conduits	Wires are encapsulated w/in pressurized conduits so that if there is an attempt to access a wire, the pressure of the conduit will change and sound an alarm.
Unicast, Multicast, Broadcast	**Unicast** – From one system to another system **Multicast** – from one system to a group of specified systems **Broadcast** – one system to all systems on a subnet. Class D addressing.
CSMA	**Carrier Sense Multiple Access** – Ethernet used as an access method to the network cable. **2 types** 1. **CSMA/CD** – Collision Detect – when using these protocols they monitor the transmission activity or carrier activity on the wire so that they can determine when to transmit. • **Contention** – Nodes have to compete for the same shared medium • **Collision** – when 2 or more frames collide and corrupts both frames. • **Back-off Algorithm** – After a collision a timer is used before can retransmit. 2. **CSMA/CA –** Collision Avoidance – access method in which each computer signals its intent to transmit data before it actually does so. **CSMA is faster than token-passing, but tokens do not have problems with collisions.** **Collision Domain** – a group of computers that are contending, or competing, for the same shared communication medium.
Polling	Where stations are configured as primary stations and others are secondary stations. At predefined intervals the primary station will ask the secondary system if it has anything to transmit. • Used mainly with mainframe environments.
ARP/RARP	**ARP** – Requesting the MAC address from the given IP address. • **ARP Table Poisoning** – altering a systems ARP table so that it contains incorrect info. It's a **masquerading** attaché because the attackers goals is to receive packets that were intended for anther computer

<table>
<tr><td></td><td><b>RARP</b> – Requesting the IP address from the given MAC address.
• <b>BOOTP</b> was created after RARP to enhance functionality.</td></tr>
<tr><td><b>Autonomous System</b></td><td>An individual network managed by a specific authority and implements its own internal routing.
• AS’s communicated through BGP</td></tr>
<tr><td><b>Multilayered switches</b></td><td>They combine D-link layer, network layer, and other layer functionalities.
• Use HW based processing power to look deeper w/in a packet to make decisions</td></tr>
<tr><td><b>Gateway</b></td><td>General term for SW running on a device that connects 2 different environments and acts as a translator b/t them or restricts interactions.
• Usually a gateway is needed when one environment speaks a different language</td></tr>
<tr><td><b>Devices and functionality</b></td><td>
<table>
<tr><th>Device</th><th>OSI Layer</th><th>Functionality</th></tr>
<tr><td><b>Repeater</b></td><td>Physical</td><td>Amplifies signal and extends networks</td></tr>
<tr><td><b>Bridge</b></td><td>D-Link</td><td>Forwards packets and filters based on MAC addresses; forwards broadcast traffic, but not collision traffic</td></tr>
<tr><td><b>Switch</b></td><td>D-Link</td><td>Provides private virtual link b/t comm. Devices, allows for VLANs, reduces traffic, and impedes network sniffing</td></tr>
<tr><td><b>Router</b></td><td>Network</td><td>Separates and connects LANs creating internetworks; routers filter based on IP addresses.</td></tr>
<tr><td><b>Gateway</b></td><td>Application</td><td>Connects different types of networks, performs protocol and format translation.</td></tr>
</table>
</td></tr>
<tr><td><b>Firewalls</b></td><td><b>Def –</b> used to restrict access to one network from another network. A “choke point” in a network b/c all communication should flow through it.
• Firewall is a type of gateway that can be a router, server, authentication server, or specialized HW device
<b>Firewall types:</b>
1. <b>Packet Filtering</b>
2. <b>Stateful Inspection</b>
3. <b>Proxy Firwalls</b>
4. <b>Application level Proxy</b>
5. <b>Circuit level proxy</b>
6. <b>Dynamic packet filtering</b>
7. <b>Kernel Proxy</b></td></tr>
<tr><td><b>Packet Filter</b></td><td>Routers using ACLs dictate acceptable access to a network. Looks at destination and source addresses, ports and services requested.
• Operates at the Network Layer. Makes decisions based on the header info only.
<b>Pros</b>
• Scaleable
• Provides high performance
• Application Independent
<b>Cons</b>
• Does not look into the packet past the header info
• Low security relative to other options
• Does not keep track of the state of a connection</td></tr>
<tr><td><b>Stateful Inspection</b></td><td>Keeps track of each conversation using a state table. Looks at the state and context of packets.
<b>Characteristics:</b>
• FW maintains a state table and track each coms channel
• Frames are analyzed at all communication layers
• Provides a high degree of security and does not introduce the performance hit that proxy FW introduce
• Scaleable and transparent to users
• Provides data for tracking connectionless protocols (UDP/ICPM)
• State and context of the data w/in the packets are stored and updated continuously.
• Considered a third generation FW
<b>Susceptible to flooding of the state table w/ bogus info</b> – it can either freeze the device or cause it to reboot. If forced to reboot it losses info on recent connections and will deny legitimate packets.</td></tr>
<tr><td><b>Proxy FW</b></td><td>Proxy is a middleman that accepts messages either entering or leaving a network, inspect them for malicious info, and when it decides its okay, passes the data on the destination computer.
• Second generation FW
• Stands b/t a trusted and untrusted network and makes the connection, each way, on behalf of the source.
• Takes a copy of each accepted packet and repackages the packet to hide the packets true origin.
• Only computer that needs a valid IP address</td></tr>
</table>

	Pros • Looks at info w/in a packet, possibly all the way up to the application layer • Provides better security than packet filtering. • Breaks connection b/t trusted and untrusted systems **Cons** • Some Proxy FW are limited to what applications it can support • Degrades traffic performance • Application-based proxy FW can have scalability issues • Breaks client/server model, which is good for security but bad at times for functionality.
Application Level Proxy	Inspect the entire packet and make access decisions based on the content of the packet. • One Application proxy is required per service. • Provides more intricate control than circuit level proxy FW • Reduces network performance • Application Layer
Circuit level Proxy	Creates a circuit b/t the client computer and the server. Looks at the header packet info and protects a wider range of protocols and services and app level proxy's but does not provide the detailed level of control. • Does not require a proxy for each and every service • Does not provide the detailed level of access control that an application proxy does • Provides security for a wider range of protocols. **SOCKS** – an example of a circuit-level proxy gateway that provides a secure channel b/t 2 computers. When a SOCKS enabled client sends a request to access a computer on the internet, the request goes to the network's SOCKS proxy server, which inspects the packets for malicious info and checks policy rules. • SOCKS server can screen, filer, audit, log, and control data flowing in and out of a protected network. • Requires clients to be SOCKS-ified w/ SOCKS client SW. • Can be resource intensive • Provides authentication and encryption features similar to other VPN protocols, but not considered a true VPN
Dynamic Packet Filtering	Receiving systems require an IP address and port number so it can respond properly so the sender must choose a dynamic port higher than 1024 when it sets up a connection. The dynamic packet filtering FW will then create an ACL that allows the external entity to communicate to the internal systems via this high port. • If this was not available option you would have to punch holes in your FW for all ports above 1024. • ACLs are dynamic in natures so once the connection is finished the ACL is removed from the list. • On connectionless protocols the connection will time out and the ACL is pulled • Fourth generation FW • Benefit is it gives you the option of allowing any type of traffic outbound and allowing only response traffic inbound.
Kernel Proxy	A 5th generation FW that when a packet arrives at the FW a new network stack is created, which is made up of only the protocol proxies that are necessary to examine this specific packet. • If an FTP packet is received only the FTP proxy is loaded into the stack and the packet is scrutinized at every layer of the stack. If anything is deemed unsafe the packet is discarded. • Faster than application layer FW b/c all of the inspection and processing is taking place in the kernel and does not need to be passed up to a higher SW layer in the OS. • It is a proxy so the connection b/t internal and external is broken. • Can perform NAT.
Screened Host	A FW that communicates directly w/ a perimeter router and the internal network
Screened subnet	FW is sandwiched b/t 2 routers and the external router applies packet filtering. The second router behind the FW redirects the traffic to the internal network and filters the traffic. • Sets up a DMZ b/t the two FWs
Shoulds of FWs	• Default action of any FW should be to implicitly deny any packets and not explicitly allowed • Any packets entering the internal network that have a source address of an internal host should be denied. Attack call **masquerading or spoofing**. • No traffic should be allowed to leave the network that does not have an internal source address. If they are being used in a DoS attack using zombies. • FWs should reassemble fragment packets before sending them on to destination so that they can evaluate the entire packet. • Deny source routing.

Disadvantages of FWs	• Security is concentrated in one spot vs. distributed approach • Can create a bottleneck for network traffic • FWs can restrict desirable services that users may want to access. • Most FWs do not do virus screening. • Provide little protection from the inside attacker.
NOS	Network Operating system – designed to control network resource access and provide the necessary services to enable a computer to interact with the surrounding network. • Built to work in a client/server model that enables resources, files, and applications to be centralized, while all users access them on servers, rather than having individual copies of those resources stored on each and every workstation. • NOS uses a redirector that points the computer to the actual requested resource.
DNS	Domain Name Server – Until 1999 IANA (Internet Assigned Number Authority) maintained and coordinated the allocation of IP addresses. After 1999 ICANN (Internet Corporation for Assigned Names and Numbers) took over responsibility of IP address block allocation, DNS mgmt, and root server system mgmt. • **Zones** – w/in DNS servers network are split into zones. The DNS server that holds the files for one of these zones is said to be the **authoritative** name server for that particular zone. Zone may contain one or more domains. • The zone files contain records that map hostnames to IP addresses, which are referred to as **resource records** • It is recommended that a **primary** and **secondary** DNS server be placed in each zone. Primary contains the actual resource records for a zone and the secondary contains copies of those records.
Directory Service	Has a hierarchical DB of users, computers, printers, resources, and attributes of each. Directory is mainly used for lookup operations, which enable users to track down resources and other users. • Most directory DB are built on the X.500 model and use the LDAP (Lightweight Directory Access Protocol) to access the directory DB • **Metadirectories** – hold top level info about the directory itself, which enables a user in one directory to locate an object in a different directory. • **Metadata** – is data about data. • **Schema** – each directory follows a schema which provides structure to the directory repository and defines how objects and their relationships are to be represented.
Extranet	Extend the bounds of the companies network to enable 2 or more companies to share common info and resources. Accommodate B2B communication.
MANs	**Metropolitan Area Network** – usually a backbone that connects LANs to each other and LANs to WANs, the internet and telecom and cable networks. • Majority of today's MANs are SONET (Synchronous Optical Network) or FDDI rings provided by telecom providers • SONET is a telecom standard for transmission over fiber optics. • SONET is self healing meaning if a break occurs on one of its lines due to a disaster it can use a backup redundant ring to ensure that transmission continues. • SONET networks can transmit voice and data over optical.
Multiplexing	Method of combining multiple channels of data over a single transmission path
ATM communication	ATM is the network evolutionary step in telecom. • Encapsulates data in fixed cells instead of the variable frame size used by earlier technologies. Provides better performance and reduced overhead for error handling • ATM is done over a SONET network • ATM is used in LAN and WAN implementations.
Dedicated links	AKA Leased line or Point to point link. Pre-established single link b/t 2 destinations.
T-Carriers	Dedicate lines that can carry voice and data info over trunk lines. Digital circuits that multiplex several individual channels into a higher speed channel.
S/WAN	Building secure FW to FW connections based on VPNS that are created w/ IPSec
CSU/DSU	Channel Service Unit/Data Service Unit – required when digital equipment will be used to connect a LAN to a WAN network. • DSU converts digital signals from routers, bridges, and multiplexers into signals that can be transmitted over the telephone company's digital lines. Ensure voltage level is correct and info is not lost during the conversion. • CSU connects the network directly to the telephone company. • CSU/DSU provides a digital interface for DTEs such as terminals, multiplexers, routers
Circuit Switching vs. Packet Switching	**Circuit switching:** • Connection oriented virtual links

<table>
<tr><td></td><td colspan="2">• Traffic travels in a predictable constant manner
• Fixed delays
• Usually carries voice oriented data
Packet switching:
• Packets can use many different dynamic paths to get to the same destination
• Traffic is usually bursty in nature
• Variable delays
• Usually carries data</td></tr>
<tr><td rowspan="11">**WAN Technolgies**</td><th>WAN Technology</th><th>Characteristics</th></tr>
<tr><td>Dedicated lines</td><td>• Dedicated, leased line that connects 2 locations
• Expensive compared to other WAN options
• Secure b/c only 2 locations are using the same media</td></tr>
<tr><td>Frame Relay</td><td>• High performance WAN protocol that uses packet-switching over public networks
• Shared media among companies
• Uses SVCs & PVCs
• Fee based on used bandwidth</td></tr>
<tr><td>X.25</td><td>• First packet switch technology developed to work over public networks
• Shared media among companies
• Lower speed than frame relay b/c of extra overhead
• International standard and used more in countries other than the US</td></tr>
<tr><td>SMDS</td><td>• Switched Multimegabit Data Service
• High speed switch tech used over public network
• Connectionless and can provide bandwidth on demand</td></tr>
<tr><td>ATM</td><td>• High bandwidth switching and multiplexing technology that has low delay
• Uses 53 byte fixed size cells
• Uses PVCs and SVCs
• Very fast b/c of the low overhead</td></tr>
<tr><td>SDLC</td><td>• Synchronous Data Link Control
• Enables mainframes to communicate with remote offices
• Provides polling mechanisms to allow primary and secondary stations to communicate.
• Based on dedicated, leased lines and used mainly for coms to IBM hosts w/in a SNA</td></tr>
<tr><td>HDLC</td><td>• High Level Data Link Control
• A data encapsulation method for synchronous serial links
• Point to point and multipoint communication</td></tr>
<tr><td>HSSI</td><td>• High Seed Serial Interface
• DTE/DCE interface to enable high speed coms (ATM, Frame) over WAN links.</td></tr>
<tr><td>VOIP</td><td>• Voice over IP
• Combines voice and data over the same IP network media and protocol
• Reduces costs of implementing and maintaining 2 different networks
• **Jittering** – when packets holding someones voice gets queued and is delayed</td></tr>
<tr></tr>
<tr><td>**Mulitservice Access**</td><td colspan="2">Technologies that combine several types of communication categories (data, video, voice) over one transmission line.</td></tr>
<tr><td>**H.323 Gateways**</td><td colspan="2">A standard that deals with video, real time audio, and data packet based transmissions where multiple user can be involved</td></tr>
<tr><td>**ISDN (Integrated Services Digital Network) Implementation**</td><td colspan="2">**BRI** – Basic rate interface – 2 B channels and 1 D channel with bandwidth of 144kbps
PRI – Primary Rate Interface – 23 B channels and 1 D Channel with bandwith of 1.544 Mbps.
BISDN – Broadband ISDN – Used w/in Telecom backbones, ATM is used to encapsulate data at the D-link layer into cells, which travel over SONET network.</td></tr>
<tr><td>**DSL**</td><td colspan="2">**Digital Subscriber Line** – provides 6 to 30 times higher bandwidth speeds than ISDN and analog technologies. Uses existing phone lines.
• Have to be w/in 2.5 miles of the CO b/c as the distance b/t residence and the CO increases the transmission rates decrease</td></tr>
</table>

	• Broadband technology and provides up to 52 Mbps speed • Offer Symmetric service which means traffic flows at the same speed upstream and downstream • Offer Asymmetric where the downstream speed is much higher than upstream
PPP	**Point to point protocol** – used to encapsulate messages and transmit them over a serial line. Used to allow TCP/IP and other protocols to be carried across dial up lines. • It is **serial connection** b/c one bit follows the one in front of it compared to **parallel** where channels of bits travel at one time. • Can use PAP, CHAP or EAP for authentication • PPP replace **SLIP (Serial Line Internet Protocol)** – an older protocol that was used for encapsulating data to be sent over serial connections. **PPP Advantages over SLIP:** • PPP implements header and data compression • PPP has error correction • PPP supports different authentication methods • PPP can encapsulate protocols other than IP • PPP does not require both ends to have an IP address assigned before data transfer
VPN Tunneling Protocols	**1. PPTP** • Designed for client/server connectivity • Sets up a sign pt to pt connection b/t 2 computers • Works at d-link layer • Transmits over only IP networks • Microsoft Protocol **2. L2F (Layer 2 Forwarding)** • Created before L2TP by Cisco • Merged with PPTP which resulted in L2TP • Provides mutual authentication • No encryption **3. L2TP** • Hybrid of L2F and PPTP • Sets up a single pt to pt connection b/t 2 computers • Works at the • D-link layer • Transmits over multiple types of networks • Combined with IPSec for security • Does not provide encryption or authentication services. • Supports TACACS+ and RADIUS **4. IPSec** • Handles multiple connections at the same time • Provides secure authentication and encryption • Supports only IP networks • Focuses on LAN to LAN communication rather than a dial up prot • Works at the network layer, and provides security on top of IP • Can work in **Tunnel Mode** – Meaning the payload and header are protected or **Transport Mode** – meaning that only the payload is protected.
PAP vs CHAP and EAP	**PAP** – Password Authentication Protocol • Sends credentials in cleartext during transmission • Decreases in use b/c it does not provide a high level of security • Supported by most networks and network access servers **CHAP** – Challenge Authentication Handshake Protocol • Used the same way is used but provides a higher degree of security • Authenticates using a challenge/response method • Used by remote users, routers and NASs to provide authentication before providing connectivity. • Not vulnerable to man-in the middle attacks because uses challenge/response throughout the connection **EAP** – Extensible Authentication Protocol – not a specific authentication mechanism, instead it proves a framework to enable many types of authentication techniques to be used during PP connections. • Extends the authentication possibilities from PAP and CHAP to other methods such as one-time passwords, token cards, biometrics, kerberos, and future mechanims
Remote Access Guidelines	• Security policy or issue specific policy should outline • Access modems should be set to answer after the 4th ring. Wardialers are often configured to

move other numbers after 2 or 3 rings.

- All access servers and modem pools should be housed in the same server room and admined by the same person/group.
- Strong 2 factor authen via RADIUS or TACACS should be implemented
- Caller ID or call back setting should be configured on the RAS
- Call back can be bypassed by call forwarding.

RAID

Redundant Array of Inexpensive Disks – technology used for redundancy and performance improvement. Combines several physical disks and aggregates them into logical arrays.

- If fault tolerance is one of the services that a RAID level is providing, parity is involved
- **Parity** – Data can be written to each disk, which works as a backup. If one drive fails, the parity data is used to rebuild a new drive and all the info is resorted.
- **Hot-swapping Disks** – Most RAID systems provide and when a drive is swapped out or added the parity data is written to each diskrebilds the data on the new disks that was just added

RAID Advisory Board (RAB) has developed these new classifications:

1. **Failure Resistant Disk Systems** – Protects against loss of data or access due to a disk failure.
2. **Failure Tolerant Disk Systems** – Protects against loss of data access due to failure of any single component and offers continuous data availability.
3. **Disaster Tolerant Disk Systems** – Two or more zones are used to provide access to stored data. These systems describe server systems that are divisible into 2 or more zones. The mechanisms w/in the zones cooperate to protect against loss of access, caused by power outage, cooling system, or component Failure

RAID Levels and Explanations

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity involved. If one volume fails, the entire volume is unusable. Used for performance only	Striping
1	Mirroring of drives. Data is written to 2 drives at once. If one fails the other drive has the exact same data available	Mirroring
2	Data striping over all drives at the bit level. Parity data is created w/ a hamming code, which identifies any errors. This level specifies the use of up to 39 disks: 32 for storage and 7 for error recovery of data. This is not used in production today	Hamming code Parity
3	Data striping over all drives and parity data held on one drive. If a drive fails it can be reconstructed from parity drive	Byte-level parity
4	Same as level 3, except data is striped at the block level instead of the byte level	Block-level parity
5	Data is written in disk sector units to all drives. Parity is written to all drives also, which ensures that there is no single point of failure	Interleave parity
6	Similar to 5 but with added fault tolerance, which is a second set of parity data written to all drives	Second parity data or double parity
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures. Combo of Level 1 & 0	Striping and Mirroring
15	Combo of level 1 and 5	

HSM and SAN

HSM – Heirarchical Storage Mgmt – provides continuous online backup functionality. Combines hard disk technology w/ cheaper and slower optical or tape juke boxes.

SAN – Storage Area Network – Storage systems are connected together to from a single backup network. Private channels or storage controllers are implemented so hosts can access the different backup devices transparently.

Clustering

Fault tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are request. Group of servers viewed logically as on server

Wireless Spread spectrum

- FCC decides upon allotment of frequencies
- **Spread spectrum** – means that something is distributing individual signals across the allocated frequencies in some fashion. Allows for more effective use of the available bandwidth, b/c sending system can use more than one frequency at a time.

2 Types:

1. FHSS
2. DSSS

FHSS

Frequency Hopping Spread Spectrum – Takes the total amt of bandwidth (spectrum) and splits into smaller subchannels.

- The signal will be traveling over one frequency and then change, or hop, to another frequency. FHSS algrorithm determines the frequency to which the signal will hop

	• Hoping is done avoid interference, so if it hops to another frequency the signal will not be affected. • Uses only a portion of the bandwidth at any one time • FHSS uses a narrow band carrier • Lower data throughput • Signal is distorted will have to be resent
DSSS	**Direct Sequence Spread Spectrum** – Applies sub-bits to a message and the sub-bits are used by the sending system to generate a different format of the data before it is transmitted. Receiving end uses these bits to reassemble the signal into the original data format. • Sub-bits are collectively called a **Chip** and the sequence of how the sub-bits are applied is **Chipping Code** • When the senders data is combined with the chip, to anyone who does not know the chipping sequence, the signal appears as random noise. Sequence is sometimes called a **pseudo-noise** sequence. • Signal is distorted still can recover • Uses all of the bandwidth continuously • Provides more security • Less affected by fading and negative affects of jumping • Spreads the signal over a wider frequency band • Sends data across all frequencies at once and has a higher data throughput.
Wireless Standards	• IEEE – Institute of Electrical and Electronics Engineers develops the wireless standards • 802.11 standard is a WLAN technology and has several variations • 802.15 standard outlines WPAN (Wireless Personal Area Network) • 802.16 standard address wireless MAN technologies. • 802.11b standard works in the 2.4 Ghz range at 11mbps and 802.11a works in the 5Ghz range at 54 Mbps.
WAP	**Wireless Application Protocol** – Not a standard instead is a market and industry driven protocol stack. WAP provides a common architecture for wireless devices to be able to communicate over the Internet. • WAP uses WML (Wireless Mark-up language) and WMLScript to present material and perform processing in the background • **WTLS** – Wireless Transport layer Security – Similar to TLS or SSL. • B/c these devices use a different set of protocols a gateway is required to translate b/t WAP and the Inet protocols and application types. • Security concern is that WTLS data will be decrypted at the service provider and then encrypted with TLS or SSL and for a second or 2 the data is not protected called a **gap in the WAP**. **WTLS has 3 classes that define authentication:** • **Class 1 = Anonymous authentication** – wireless device and server do not authenticate each other. • **Class 2 = Server Authentication** – Server authenticates to the wireless device • **Class 3 = Two way client and server authentication** – the server and the wireless device authenticate to each other.
WLAN Components	**Access Point** – a WLAN transceiver. Are in a fixed locations throughout a network and work as communication beacons. **Infrastructure WLAN** – AP used to bridge wireless and wired networks. Used to extend an existing wired network. **Ad hoc WLAN** – Ther are no APs and wireless devices communicate to each other through peer to peer **Channel** – For a wireless device and AP to communicate must be configured to communicate over the same channel. **SSID** – Service Set ID – Used to sement different WLANs. Wireless Device can authenticate in 3 ways: **1.** **OSA** – Open system authentication – does not require the wireless device to prove to the AP it has a specific Cryptographic key. Usually only needs to have SSID. **2.** **SKA** – Shared Key Authentication – AP will send a random value to the devices and the device will encrypt this value with its key and send it to the AP. AP will decrypt and extract and if it's the same value they are authenticated. • Based on the WEP protocol

CISSP STUDY GUIDE

6. Cryptography

Topic	Description
Cryptography	**Def** – Method of storing and transmitting data in a form that only those it is intended for can read and process. Considered a science of protecting info by encoding it into an unreadable format. Practiced by **Cryptographers.** • **Cryptanalysis** are practitioners of **cryptanalysis**, the are and science of breaking Ciphertext. • **Cryptology** is the branch of mathematics encompassing both cryptography and cryptanalysis and its practitioners are **cryptologists.**
Terminology	• **Plaintext** – A message is plaintext or sometimes called cleartext. • **Encryption** – Process of disguising a message to hide its substance is encryption. • **Decryption** – Process of turning Ciphertext back into plaintext.. • **Cryptographic algorithm** – also called a **cipher** is the mathematical function used for encryption and decryption • If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a **restricted algorithm.** • Restricted algorithms are woefully inadequate by today's standards. A large or changing group of users cannot use them, because every time a user leaves the group everyone else must switch to a different algorithm. • **Key** – is a value that is made up of a large sequence or random bits. • An algorithm contains a **Keyspace**, which is a range of values that can be used to construct a key. Larger the keyspace, more available values can be used to represent different keys and the more random keys the harder it is for an intruder to figure out. • Encryption algorithm should use the entire keyspace and choose the values to make up the keys as randomly as possible • **Key clustering** – Instance when 2 different keys generate the same ciphertext from the same plaintext.
Goals of Cryptosystems	2. **Confidentiality** – unauthorized parties cannot view info 3. **Authentication** – should be possible for the receiver of a message to ascertain its origin; intruder should not be able to masquerade as someone else 4. **Integrity** – Should be possible for the receiver of a message to verity that it has not been modified in transit; intruder should not be able to substitute a false message for a legitimate one 5. **Nonrepudiation** – A sender should not be able to falsely deny later that he sent a message
Strength of the Cryptosystem	**Strength** – of the encryption method comes from the algorithm, secrecy of the key, key length, initialization vectors, and how they work together. • Refers to how hard it is to figure out the algorithm or key, whichever is not made public. • Correlates to the amt of necessary processing power and time it takes to break the key or figure out the value of the key. • **Work factor** – an estimate of the effort it would take an attacker to penetrate an encryption method.
Types of Ciphers	1. **Substitution cipher** – Replaces bits, characters, or blocks of characters with different bits, characters, or blocks • **Monoalphabetic substitution cipher** – Uses only one alphabet to perform substitution. • **Polyalphabetic substitution cipher** – Uses multiple alphabets at a time to perform substitution. • **Caesar Cipher** – each letter is replaced w/ the letter three places beyond it in the alphabet and is referred to as a shift alphabet. 2. **Transposition cipher – AKA Permutation –** rearranges the bits, characters, or blocks of characters to hid the original meaning. • Key determines the positions that the characters are moved to. • Simple substitution and transposition ciphers are vulnerable to **Frequency Analysis** attacks. • More complex algorithms usually use more than one alphabet for substitution and permutation, which reduces the vulnerability to frequency analysis. 3. **Running key cipher** – could use a key that does not require an electronic algorithm and bit alterations, but clever steps in the physical world around you. Spy novel type cipher 4. **Concealment cipher** – i.e. deciding every 3rd word written is the message. Spy novel type cipher.
Steganography	Method of hiding data in another media so that the very existence of the data is concealed. Mainly used by hiding messages in graphic images. Least significant bit of the image can be replaced with bits of the secret message. • Can also be hidden in wave file or unused spaces on a hard drive or sectors marked as unusable.

Governments Involvement w/ cryptography	• In the US the governments cryptographic agency, the NSA was granted the power to regulate the export of cryptographic mechanisms and equipment • **Clipper Chip** – 1993 the US government proposed placing their own encryption chip in every American made comms device. • Each chip has a unit key, which is used to encrypt a copy of each user's session key, not the message itself. • Sending clipper chip generates and sends a LEAF (Law Enforcement Access Field) value included in the transmitted message. This field value contains the serial number of the clipper chip use to encrypt the message. This is how the law enforcement knows which unit key to retrieve. • Unit key is split into 2 pieces and kept in different DB maintained by 2 different escrow agencies. **Weaknesses in the Clipper Chip** • The skipjack algorithm, which clipper is based on, was never publicly scrutinized and tested • An 80 bit key is weak • A 16 bit checksum can be defeated • The clipper chip ID tagged and identified every communication session.
Kerckhoffs Principle	The only secrecy involved w/ cryptography system should be the key. The algorithm should b e publicly known.
Key Escrow	Keys are split into 2 sections and are given to 2 different escrow agencies to maintain. • For an officer to access data that is encrypted he must get a court order to request the unit key. • Outlines in the US Escrow Encryption Standard. • **Fair Cryptosystem** – uses software instead of hardware and would require 2 parts of a private key held by 2 different entities.
Symmetric Algorithms	**AKA Secret keys** – both parties will be using the same key for encryption and decryption. Relies on each user to keep the key a secret and properly protected. • Equation used to calculate the number of symmetric keys need is: N(N-1)/2 = number of keys • Key distribution is done through an **Out of band method** such as saving it on a floppy and walking it over to the other users desk. • Provide **Confidentiality**, but not authentication or Nonrepudiation. • No way to prove who sent the message if 2 people are using the same keys. • Difficult to uncover data that is encrypted with a symmetric algorithm if a large key size was used. **Strengths:** • Much faster than asymmetric • Hard to break if using a large key size **Weaknesses:** • Requires a secure mechanism to deliver keys properly • Each pair of users needs a unique pair of keys, so the number of keys grows and key mgmt can become overwhelming. • Provide confidentiality, but not authenticity or Nonrepudiation. **Symmetric Algorithms** • DES • 3DES • Blowfish • IDEA • RC4, RC5, RC6 • AES **2 types of Symmetric algorithms:** **1. Block cipher** **2. Stream cipher**
Asymmetric Algorithms	**AKA Public Key Cryptography** – each entity has different keys that are mathematically related. If the message is encrypted by one key the other key is required to decrypt. • Public key can be know by everyone and the private key must only be known and used by the end owner. • Authentication is obtained by the entity encrypting the message with there private key and the receiver will decrypt will public key and verify who it came from. Does not provide confidentiality. Called **Open message Format** b/c anyone can read the message by using the senders public key. • Confidentiality is obtained by the sender encrypting the message with the receivers public key

	and decrypted by the receivers private key. Called **Secure Message Format**. • For a message to provide confidentiality and authentication, called **Secure and Signed Format**, the sender would encrypt with there private key and then encrypt with the receivers public key. **Strengths:** • Better key distribution than symmetric systems • Better scalability than symmetric systems • Can provide authentication and nonrepudiation **Weaknesses:** • Works much more slowly than symmetric systems • Mathematically intensive tasks **Asymmetric Algorithms** • RSA • ECC – Elliptic Curve Cryptosystem • Diffe-Hellman • El Gamal • DSA – Digital Signature Algorithm • Knapsack
Block Cipher	Used for encryption and decryption purposes and the message is divided into blocks of bits, usually 64 bits. These blocks are then put through substitution, transposition, and other mathematical functions, one block at a time. • Properties of a cipher should contain confusion and diffusion • Confusion – complexity of the algorithm and not knowing the key value • Diffusion – accomplished by putting the bits w/in the plaintext through many different functions so they are dispersed throughout the algorithm. • Block cipher has 2 layers of 4-bit substitution boxes called **S-boxes** – substitution boxes. • Each S-box contains a lookup table that instructs how the bits should be encrypted. The key that is used in the encryption process dictates what S-boxes are used and in what order. • Each S-box can have different types of functions, mathematical formulas, and methods to be performed on each bit. • Key provides the confusion, b/c the attacker does not know which S-boxes would be used. • The permutations that happen on the bits are diffusion. • Strong and efficient block cryptosystems use random key values so an attacker cannot find a pattern as to which S-boxes are chosen and used. • **Used in SW implementations**
Stream Cipher	Treats the message as a stream of bits and performs mathematical function on them individually. When using a stream cipher the same plaintext bit will be transformed into a different ciphertext bit each time it is encrypted. • Some stream ciphers use a **Keystream generator**, which produces a stream of bits that is XORed with the plaintext bits to produce ciphertext • **XORed** – an operation that is applied to 2 bits. When combining them if both bits are the same the result is zero (1 + 1 = 0). If the bits are different from each other the result is 1 (1+0 = 1) • If the cryptosystem were only dependent upon symmetric stream algorithm, an attacker could get a copy of the plaintext and resulting ciphertext, XOR them together and find the keystream to decrypt other messages. Using a Key fixes this. • Key is applied to the keystream generator and creates randomness. The key is a random value input into the stream algorithm. • Both sending and receiving end must have the same key to generate the same keystream. **Strong and effective stream cipher has:** • Long periods of no repeating patterns w/in keystream values • Statistically unpredictable keystream • Keystream not linearly related to the key • Statistically unbiased keystream (as many 0s as 1s) • **Suitable for HW implementations**
DES	**Data Encryption Standard –** A block symmetric encryption algorithm using 64 bit blocks (56 bits is the true key and 8 bits used for parity) • 1974 IBM submitted **Lucifer** which used a 128 bit algorithm. NSA modified the key size to 64 (8 bits for parity and 56 for key length). This became DES.

	• A block is made up of 64 bits and is divided in half, and each character is encrypted one at a time. • Put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key . The result is a 64bit block of ciphertext.
4 DES Modes of Operation	1. **ECB** – Electronic Code Book Mode – operates like a code book where 64 bit data block is entered into the algorithm with a key, and a block of ciphertext is produced. • For a given block of plaintext and a given key, the same block of ciphertext is always produced • Not all messages end in 64bit blocks so ECB incorporates padding to address problem • **Mode is used for small amounts of data like encrypting and protecting encryption keys.** • Because this works w/ blocks independently, data w/in a file does not have to be encrypted in a certain order. • Useful in DB b/c any record or table can be added, encrypted, deleted, or decrypted independent of any other table or record. • Used for challenge response encryption and some key mgmt tasks • Used to encrypt PINs in ATM machines • Not used to encrypt large amts of data because the patterns show since no **Chaining** is used. 2. **CBC** – Cipher Block Chaining Mode **–** does not reveal a pattern b/c each block of text, the key, and the value based on the previous block is processed in the algorithm and applied to the next block of text and gives a more random result of ciphertext. • Ciphertext from the previous block is added to the plaintext of the next block. • Each block of text is dependent upon all blocks before it. 3. **CFB** – Cipher Feedback Mode – The ciphertext from the previous block of data is inputted into the algorithm to generate random values and the random values are processed with the current block of plaintext. • CFB mode emulates a stream cipher by using a keystream generator. • Used when encrypting individual characters. 4. **OFB** – Output Feedback Mode – Like CFB but is functioning like a stream cipher by generating a stream of random binary bits to be combined with the plaintext to create ciphertext. The ciphertext is fed back to the algorithm to form a portion of the next input to encrypt the next stream of bits.
3DES	Uses 48 rounds in its computation and is 2^{56} times stronger than DES. • Can take up to 3 times longer than DES to perform encryption and decryption. • symmetric algorithm **3 modes of 3DES:** 1. **DES-EE3** – Three keys are used and data is encrypted, encrypted, and encrypted 2. **DES-EDE3** – Uses three different keys, and it encrypts, decrypts, and encrypts data 3. **DES-EEE2 & DES-EDE2** – uses 2 keys and same as the previous mode, but the first and the third operation use the same key.
IDEA	**International Data Encryption Algorithm** – a block cipher symmetric algorithm and operates on 64-bit blocks of data. The 64bit data block is divided into 16 smaller blocks and each has 8 rounds of mathematical functions performed on it. • Key is 128bits long • Offers modes similar to DES but much harder to break • Used in PGP encryption SW.
Blowfish	A block cipher that works on 64bit blocks of data. • Key length can be 448 bits • Goes through 16 rounds of cryptographic functions.
RC5	Block cipher symmetric algorithm that has a variety of parameters it can use for block size, key size, and the number of rounds used. • Created by Ron Rivest • Block sizes are usually 32,64,128bits • Key size goes up to 2048 bits
RSA	Can be used for digital signatures, key exchange, and encryption. • Developed by Ron Rivest, Adi Shamir, and Leonard Adleman. • Public key algorithm • Security comes from the difficulty of factoring large numbers • Public and private keys are functions of a pair of large prime numbers and the activities

required to decrypt a message from ciphertext to plaintext is comparable to factoring a product into 2 prime numbers.

- Using its one-way function, RSA provides encryption and signature verification, and the inverse direction performs decryption and signature generation.
- Used with SSL

One-Way Function

A mathematical function that is easier to compute in one direction than in the opposite direction.

- **What all asymmetric algorithms are based on.**
- Factoring of two large prime numbers
- Easy to multiply two prime numbers to come to a value, but hard find the to the two prime numbers that calculated the value.
- When an attack occurs it is not trying every key value, but trying to factor the large number which will give the attacker the private key.
- When a user encrypts a message with a public key, this message is encoded with a one-way function. Function supplies a trapdoor, but the only way the trapdoor can be taken advantage of is if it is known about and the correct code applied. Private key provides this.

El Gamal

A public key algorithm that can be used for digital signatures, encryption, and key exchange.

- Based on calculation discrete logarithms in a finite field

ECC

Elliptic Curve Cryptosystem – Provides the same functionality as RSA, but is much more efficient.

- Provides encryption functionality requiring a smaller percentage of the resources required by RSA, and other algorithms, so it is used in wireless devices and cellular phones.
- Uses a smaller key size than RSA, but provides the same level of protection.

Hybrid Encryption Methods

Asymmetric and Symmetric together – Public key cryptography uses 2 keys generated by an asymmetric algorithm for protection encryption keys and key distribution, and a secret key is generated by s symmetric algorithm and used for bulk encryption.

- Secret key is used to encrypt the actual message
- Public keys are used to encrypt the secret key for key distribution.

Session Key

A secret key that is used to encrypt messages b/t 2 users. Only good for one communication session b/t users.

- 2 computers agree on the encryption algorithms that will be used and exchange the session key that will be used for data encryption.
- **Some keys are used to encrypt data, and others are used to encrypt keys. These keys must be kept separate from each other and neither should try to perform the other keys job. Reduce brute force attacks.**

Diffie-Hellman Key Exchange

Originated the whole public key/private key concept.

- The Algorithm is used for key distribution and cannot be used to encrypt/decrypt messages or for digital signatures.

Characteristics b/t symmetric and asymmetric

Attribute	Symmetric	Asymmetric
Keys	One key is shared b/t 2 or more entities	One entity has a public key and the other entity has a private key
Key exchange	Out of band	Symmetric key is encrypted and sent with message; thus the key is distributed by inbound means
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security service provided	Confidentiality	Authentication and Nonrepudiation

PKI

Public Key Infrastructure – An ISO authentication framework that uses public key cryptography and X.509 standard protocols.

- Set up to enable authentication to happen across different networks and the Internet.
- Particular protocols and algorithms are not specified, hence it's a framwork
- Provides authentication, confidentiality, Nonrepudiation, and integrity of the message exchanged.
- A hybrid system
- Each person who wants to participate in a PKI requires a **digital certificate** – a credential that contains the public key for that individual along with other identifying info.
- Certificated is created and signed (digital signature) by a trusted third party or **CA**.
- When the CA signs the certificate, it binds the individuals identity to the public key and the CA takes liability for the authenticity of that public key.

CA's	A trusted organization that maintains and issues digital certificates. • When a person requests a certificate, the **RA** (Registration Authority) verifies that individuals identity and passes the certificate request off to the CA. • CA constructs the certificate, signs it, delivers it to the requestor, and maintains the certificate over its lifetime • When another person wants to communicate with this person, the CA will vouch for the persons identity • Many browsers have several well known CAs configured by default but it is handled in the background. • **CRL** – Certificate Revocation List – a list of every certificate that has been revoked. Certificate may be revoked b/c the private key was compromised or the CA discovered the certificate was issued to the wrong person. - **Certification Hierarchies** – multiple CA's orgranized into groups - **Root Authority** – most trusted. - Root certificate is self signed - Root CA issues certificates only to other CA's in the hierarchy which are called **subordinate CA's**. Subordinates then issue certificates to user and other entities. - CA's can also cross certify one another. Where each CA signs the other certificate so each certificate has 2 issuing authorities. **Bridge CA** – a root CA that is at the top of the hierarchies of 2 or more different PKIs
Certificates	Mechanism used to associate a public key with a collection of components sufficient to uniquely authenticate the claimed owner. • CA uses X.509 standard for creating certificates, which dictates the different fields used in the certificate and valid values that can populate those fields. • Certificate includes serial number, version number, identity info, algorithm info, lifetime dates, and the signature of the issuing authority.
Registration Authority	Acts as a middle man b/t the user and the CA. RA cannot issue certificates but will verify all necessary identification info before passing request to CA.
The process to issue certificates in a PKI:	1. A user requests a certificate 2. A key pair is generated. User signs the public key (which contains user info) with the private key to ensure that the user actually owns the private key associated with that public key. 3. Public key is sent to the CA 4. CA verifies the signature and identification info on the public key. 5. CA signs the user's public key with the CA's own private key to create a certificate. 6. The certificate is sent back to the user. 7. The user verifies the key and the CA's digital signature to ensure the key wasn't altered by the CA or in transit. 8. Certificate is published (by the user or by the CA).
Certificate Store	Certificates, revocation lists, and certificate trust lists are saved in this location. Generally a location on the local hard disk of the computer that requested it or that was used by a user to request it.
PKI Supplies the following Services	**1. Confidentiality** **2. Access Control** **3. Integrity** **4. Authentication** **5. Nonrepudiation**
Message Integrity	• Parity bits have been used in protocols to detect modifications in streams of bits as the are passed form one computer to another, but parity bits usually can only detect unintentional medications (spike in power, interference/attenuation). Cannot identify if modified by an intruder • Hash algorithms are required to detect intentional and unintentional unauthorized modifications to data.
One-way Hash and MAC	**Def** – a function that takes a variable length string, a message, and produces a fixed length value calle a hash value that represents that original data. • Hash value is also called a **message digest** • A sender would calculate a hash value for the message and append to the message. When the receiver gets it she performs the same hash function and compares the results • Not a secret. Secrecy is in its one-wayness. • Function is only run in one direction not the other. • Takes place w/out any keys • Just hashing is vulnerable to interception, changing the message, and rehashing with not the same hash value that the sender appended.

<table>
<tr><td></td><td>• Using **MAC (Message Authentication Code)** a symmetric key would be concatenated with the message and the result is put through a hashing algorithm. MAC value is generated and the MAC value is then appended to the message. If intercepted the attacker would not have the symmetric key to create the MAC value
• MAC provides **Data origination authentication AKA system authentication**. This is different than user authentication which would require the use of a private key. **DES uses MAC for data origin authentication.**</td></tr>
<tr><td>**One-way hashing function vs. MAC**</td><td>**One-way Hashing:**
• Provides integrity of a message, not confidentiality or authentication
• The result of a one-way has is a hashing value, AKA message digest
• Hashing value is used in hashing to create a fingerprint for a message
Message Authentication Code:
• A symmetric key is combined with the message before being put through a hashing algorithm
• Provides integrity and data origin authentication.</td></tr>
<tr><td>**Digital Signatures**</td><td>A hash value that has been encrypted with the sender's private key.
• Provides authentication and Nonrepudiation
• First uses a one-way hash function on the message and then the sender encrypts that hash value with his private key. When receiver gets they will perform the hashing function on the message and get a hash value. Then decrypt the sent hash value with the senders public key and compare.</td></tr>
<tr><td>**Different security services of cryptography**</td><td>1. A message can be encrypted, which provides confidentiality
2. Message can be hashed, which provides integrity
3. Message can be digitally signed, which provides authentication, nonrepudiation, and integrity.
4. Message can be encrypted and digitally signed which provides confidentiality, authentication, nonrepudiation, and integrity</td></tr>
<tr><td>**DSS**</td><td>**Digital Signature Standard** – NIST proposed this federal standard and was developed for federal departments and agencies, but most vendors use.
• Federal government requires the use of DSA (digital signature algorithm), RSA, or ECDSA (Elliptic curve digital signature algorithm), and SHA (Secure Hash algorithm)
• **SHA** – creates a 160 bit message digest output, which is inputted into one of the 3 mentioned digital signature algorithms. SHA is used to provide integrity of the message and the other algorithms are used to sign the message</td></tr>
<tr><td>**Characteristics of a good Hash function**</td><td>• Be **collision Free** – ensures that a hash algorithm does not create the same hash value for 2 or more messages
• Computed over the entire message
• Hash should be a one-way function so that messages are not disclosed by their values
• Be resistant to birthday attacks, meaning an attacker should not be able to find 2 messages with the same hash value</td></tr>
<tr><td>**Different Hashing algorithms available**</td><td><table>
<tr><th>Algorithm</th><th>Description</th></tr>
<tr><td>**Message digest 2 (MD2)**</td><td>One-way function. Produces a 128 bit hash value. Much slower than MD4 or MD5, but not weaker</td></tr>
<tr><td>**Message digest 4 (MD4)**</td><td>One-way function. Produces a 128bit hash value. Used for high speed computation in SW implementations</td></tr>
<tr><td>**Message digest 5 (MD5)**</td><td>One-way function. Produces a 128bit hash value. More complex than 4 by adding a 4th round of operations</td></tr>
<tr><td>**HAVAL**</td><td>One-way function. Variable length hash value. Modification of MD5 that processes blocks twice the size of MD5 and provide more protection.</td></tr>
<tr><td>**SHA**</td><td>One-way function. Produces a 160bit hash value. Used w/ DSA</td></tr>
</table></td></tr>
<tr><td>**Attacks against One way hash**</td><td>**Birthday Attack** – Higher probability of finding two people in a room with the same birthday than someone with your birthday.
• Output of a hashing algorithm is **n** and to find a message through a brute force attack that results in a specific hash value would require 2^n random messages.
• Finding a messages that hash to the same value would only require 2^n/2
• So MD5 using a 128 bit output will require 2^64computations to break</td></tr>
<tr><td>**One-time Pad**</td><td>A perfect encryption scheme b/c it is unbreakable by brute force by using the pad only once.
• A one-time pad uses a truly nonrepeating set of random bits that are combined bitwise using XOR function. The bits of the message are XORed to the bits in the pad to generate ciphertext.
• Random pad is the same size as the message and is used only once. B/c the entire pad is random and as long as the message it is said to be unbreakable with infinite resources.
• After use the one-time pad is destroyed</td></tr>
<tr><td>**Rules for keys and key**</td><td>• Key length should be long enough to provide the necessary level of protection</td></tr>
</table>

mgmt	• Keys should be stored and transmitted by secure means • Keys should be extremely random and use the full spectrum of the keyspace • Keys lifetime should correspond with the sensitivity of the data it is protecting. (less secure data may allow for a longer key lifetime, whereas more sensitive data might require a shorter key lifetime) • The more the key is used, the shorter its lifetime should be • Keys should be backed up or escrowed in case of emergencies • Keys should be properly destroyed when their lifetime comes to an end.
Link vs. End to End Encryption	**Link Encryption** – encrypts all data long a specific coms path. User information, header, trailers, addresses, and routing data are all encrypted. • The only data that is not encrypted is the D-link control messaging info, which includes instructions and parameters that eh different link devices use to synchronize communication methods • Provides extra protection against packet sniffers and eavesdroppers. • Does expose the packets headers at each hop that has to decrypt it. • Happens at the lower end of the OSI model (d-link and physical) • Referred to as **traffic-flow security or Online encryption.** **Advantages of Link Encryption** • All data is encrypted, including headers, addresses, and routing info • Users do not need to do anything to initiate; it works at a lower layer in the OSI model **Disadvantages of Link** • Key distribution and mgmt is more complex b/c each hop device must receive a key, and when the keys change, each must be updated • Messages are decrypted at teach hop **End-to-End Encryption** – headers, addresses, routing and trailer info are not encrypted, enabling attackers to learn more about the a captured packet and where it is headed. • Packets do not need to be decrypted at each hop • Encryption at the higher laeyers **Advantages of End to End** • Protects info from start to finish throughout the network • Provides flexibility to the user in choosing what gets encrypted and how • Higher granularity of encryption is available b/c each application or user can use a different key • Each hop computer on the network does not need to decrypt **Disadvantages** • Headers, addresses, and routing info are not encrypted • Destination system needs to have the same encryption mechanisms t properly decrypt the message.
HW vs. SW cryptography systems	• SW is less expensive and provides a slower throughput than HW • SW can be more easily modified and disabled compared to HW • HW is faster and performs high end encryption functions
Email Standards	Standards are necessary b/c they help ensure interoperability among vendor products **1. MIME** – Multipurpose Internet Mail Extension – technical specification indicating how multimedia and email attachments are to be transferred. **2. S/MIME** – Secure MIME – standard for encrypting and digitally signing electronic mail that contains attachments and for providing secure data transmissions. • Provides confidentiality through encryption, integrity through the user's hashing algorithm, authentication through the use of X.509 public key certificates, and nonrepudiation through cryptographically signed messages **3. PEM** – Privacy Enhanced Mail – an Inet standard to provide secure email over the Inet and for inhouse communication infrastructures. • Protocols w/in PEM provide authentication, message integrity, encryption, and key mgmt. • Provides compatibility w/ many types of key mgmt processes and symmetric/public key encryption **Components that can be used with PEM:** • Messages encrypted with DES in CBC mode • Public key mgmt provided using RSA • X.509 standard used for certification structure and format **4. MSP** – Message Security Protocol – Military's PEM

	5. **PGP** – Pretty Good Privacy – uses RSA public key encryption for key mgmt and IDEA symmetric cipher for bulk encryption of data. - Provides confidentiality by encryption and integrity using the MD4 hash, authentication through public key certificates, and nonrepudiation through the use of signed messages. - Uses its own type of digital certificates. - Does not use a CA but uses a community of trust - **Key Ring** – collection of signed public keys in a file that an individual has received from other users
HTTP	**Hypertext Transport Protocol** – Protocol of the Web and HTTP sits on top of TCP/IP - TCP/IP handles the connection and HTTP delivers the payload - HTTP is a stateless protocol, which means the client and the web server make and break a connection for each operation and has no memory of prior connections
S-HTTP	**Secure HTTP**- First the server will query the client to determine type of encryption method to use and the 2 agree upon it. Client sends the server its public key and the server generates a session key, encrypts it with the clients public key and sends it back - Protects each message sent b/t 2 computers. - It is a stateful protocol, b/c of the overhead required to re-handshake the connection.
HTTPS	Protects the communication channel b/t 2 computers, messages and all. - Uses SSL and HTTP to provide a protected circuit b/t a client and a server.
SSL	**Secure Socket Layer** – protects a communication channel instead of individual messages. Uses public key encryption, and provides data encryption, server authentication, message integrity, and optional client authentication. - Same as S-HTTP with using a session key. - Provides security for the connection, but not for the data once it is received - Works at the transport laeyr
SET	**Secure Electronic Transaction** – a security technology proposed by Visa and Mastercard to allow for more secure credit card transaction possibilities than what is currently available - A user must enter their credit card number into their electronic wallet SW and this info will be stored on the hard drive or on a smart card. The SW will then create a public an private key used specifically for encrypting financial info before it is sent.
Cookies	Since HTTP is a stateless protocol and has no memory of prior connections, cookies are used by saving prior connection data to the client's computer. - Cookies can also be used as a timestamp to ensure that a session b/t a user and a server is restricted to a specific length of time.
SSH	**Secure Shell** – functions as a type of tunneling mechanism that provides terminal like access to remote computers. SSH is a program that can be used to log into another computer over a network - Provides authentication and secure transmissions over public networks - Use session keys via Diffie-Hellman algorithm
IPSec	**Internet Protocol Security** – a method of setting up a secure channel for protected data exchange b/t 2 devices. **2 security protocols used:** 1. **AH** – Authentication Header – the authentication protocol using MAC, which also provides data integrity 2. **ESP** – Encapsulating Security Payload – an authentication and encryption protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity. ESP is used with VPN instead of AH. **2 modes of IPSec:** 1. **Transport mode** – where the payload of the message is protected. 2. **Tunnel Mode** – where the payload and thre routing and header info is also protected - **SA** – Security Association – Each device will have at least one SA for each session. SA is critical and is a record of the configurations of the device needed to support an IPSec connection - SA contains the authentication and encryption keys, agreed upon algorithm, key lifetime, and the source IP address. - SAs are directional so a device will have one SA for outbound traffic and a different SA for inbound. - **SPI** – Security Parameter Index – keeps track of the different SAs. - IPSec is a framework and does not dictate hashing or encryption algorithms to use. - **IKE** – Internet Key Exchange – defacto standard for IPSec key exhanges. A combination of ISAKMP and OAKLEY protocols.

	• ISAKMP – Internet Security Association and Key Mgmt Protocol – an authentication and key exchange architecture that is independent of the type of keying mechanisms used. • OAKLEY protocol carries out the negotiation process. • All work at network layer
Attacks	**Passive Attacks** – hard to detect b/c the attacker is not effecting the protocol. Examples are Eavesdropping, network sniffing, and capturing data as it passes. Used to gather data prior to an active attack. **Active Attacks** – Altering messages, modifying system files, and masquerading are examples b/c the attacker is actually doing something.
Ciphertext-Only Attack	The attacker obtains ciphertext of several messages, with each message being encrypted using the same encryption algorithm. • Attackers goal is to discover the key • Most common attack b/c easy to get ciphertext, but hardest attack to be successful at.
Known-Plaintext Attack	The attacker has the ciphertext of several messages, but also the plaintext of those messages. • Goal is to discover the key by reverse-engineering and trial/error attempts
Chosen Plaintext Attack	The attacker not only has access to the ciphertext and associated plaintext for several messages, be he also chooses the plaintext that gets encrypted. • More powerful than a known-plaintext attack b/c the attacker can choose specific plaintext blocks to encrypt, ones that might yield more info about the key.
Chosen-Ciphertext Attack	Attacker can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. • This is a harder attack to carry out, and the attacker would need to have control of the system that contains the cryptosystem
Adaptive Attacks	Each of the attacks have a derivative with the word adaptive in front of it. This means that an attacker can carry out one of these attacks, and depending what is gleaned from the first attack, the next attack can be modified. This is the process of reverse-engineering or cryptanalysis attacks.
Man-in-the-Middle Attack	**Steps** 1. A users sends their public key to another user and the attacker intercepts this key and sends the intended recipient the attackers public key. 2. The recipient sends their key to the other user and the attacker intercepts and sends the user the attacker key. 3. The attacker can now decrypt the message with his private key, read the message, and then encrypt with the recipients public key. • Public keys are often kept on a public server and an attacker an intercept a request or can substitute his public key on a DB. • SSL has been know to be vulnerable by the attacker injecting themselves at the beginning of the authentication phase and obtaining both parities keys. • Using digital signatures during the session-key exchange can circumvent this attack, because the attacker does not have the private key of the CA or the users.
Dictionary Attacks	Running a number of words through a one-way hash function and storing them. Once the password file is obtained from a system the attacker runs a compare against his file of one-way hashed passwords to find passwords.
Replay attack	When an attacker captures some type of data and resubmits it with the hopes of fooling the receiving device into thinking it is legitimate info. Many times this is the authentication data. • Timestamps and sequence numbers are 2 countermeasure to the replay attack
Side Channel Attacks	• Detecting how much power consumption is used for encryption/decryption (fluctuation of voltage) • Intercept the radiation emissions • Process of looking around the cryptosystem, or physical implmentation, instead of defeating it mathematically.

7. Business Continuity Planning

Topic	Description
Various Backup Types	1. **Incremental Backup** – A procedure that backs up only those files that have been modified since the previous backup of any sort. It does remove the archive attribute. • Finish more quickly than differential backups, but they take longer to restore b/c removing the archive attribute requires each incremental backup to be restored since the last full backup.

	2. **Differential Backup –** A procedure that backs up all files that have been modified since the last full backup. Does not remove the archive attribute. 3. **Full Backup** – Backups up all files, modified or not, and removes the archive attribute.
Disk Shadowing	Uses 2 physical disks and the data is written to both at the same time for redundancy purposes.
Disk Duplexing	Has more than one disk controller. If one disk controller fails the other is ready and available.
Electronic Vaulting	• Copy of modified file is sent to a remote location where an original backup of the file is stored • Transfers bulk backup info • Batch process of moving data
Remote Journaling	• Moves the journal or transaction log to a remote location, not the actual file • Parallel processing of transactions to an alternate site • Communication line used to transmit data as it is generated
Points	• A BCP is created in advance to minimize loss and ensure availability of critical systems • BCP ensures continuity of critical business functions and provides rapid recovery to recduce the overall impact of a disaster or disruption • BCP provides procedures for emergency responses, extended backup operations, and post disaster recovery • Should be an enterprise wide plan and each individual org should also have its own DRP • Executive mgmt should support and perform the final approval of the plan. Senior mgmt should identify and prioritize the critical missions of the company • Executives may be held liable if proper BCPs are not developed and used • Threats can be natural, manmade or technical • Continuity planning involves identifying critical resources, identifying potential threats and possible damages, and developing plans to respond to those threats • Steps of recovery planning include initiating the project, performing BIA, developing a recovery strategy, developing a recovery plan, implementing, testing, and maintaining • Project initiation phase includes getting mgmt support, developing the scope of the plan, and securing funding and resources • BIA is one of the most important first steps in planning. Qualitative and quantitative data needs to be gathered, analyzed, interpreted, and presented to mgmt. • Executive commitment and support are the most critical elements in developing the BCP • A business case must be presented to gain executive support. Done by explaining regulatory and legal requirements etc • Plans should be prepared by the people who will actually carry them out • Planning group should be made up of representatives from all dept. or org. units • DR and continuity planning should be brought into normal business decision making procedures • Loss criteria for disaster are much more than dollar. Can be operational, loss of reputation and public confidence, loss of competitive advantage, etc. • Survey should be developed and given to the most knowledgeable people to obtain info pertaining to a company's risk and recovery procedures • Plans scope can be determined by geographical, organizational, or functional means • Hot site is fully equipped and can be up and running in a couple of hours • Warm site does not have computers, but some peripheral devices. • Cold site is just a shell of a building with power, raised floors and utilities. • When returning to the original site, the least critical organizational units should go back first. • Important part is to communicate requirements and procedures to all employees • Checklist testing is when copies of the plan are handed out to each functional area to ensure that the plan properly deals with their needs and vulnerabilities • Structured walk through test is when representatives from each functional area get together and walk through the plan from beginning to end • Simulation test is when a practice execution of the plan takes place. A specific scenario is est. and the simulation continues up to the point of actual relocation to the alternate site. • Parallel test is when some systems are actually run at the alternate site. • Full interruption test is when regular operations are stopped and processing is moved to the alternate site

CISSP STUDY GUIDE

Ch 8 Law, Investigation and Ethics

Topic	Description
Organizations that have published Ethical behavior	1. **ISC2** 2. **Computer Ethics Institute** – a non profit org. that works to help advance technology by ethical means. 3. **IAB** – Internet Architecture Board – a coordinating committee for Internet design, engineering and mgmt. • The IAB has 2 task forces: IETF (Internet Engineering Task Force) and IRFT (Internet Research Task Force). 4. **GASSP** – Generally Accepted System Security Principles – Committee seeks to develop and maintain GASSP and guidance from security professionals.
IAB Acts considered unethical	1. Purposely seeking to gain unauthorized access to Internet resources 2. Disrupting the intended use of the Internet 3. Wasting resources (people, capacity, and computers) through purposeful actions 4. Destroying the integrity of computer based info 5. Compromising the privacy of others 6. Involving negligence in the conduct of Internet-wide experiments
Motive, Opportunity, and Means	**Motive** – is the who and why of a crimes – Why was it committed and by who. **Opportunity** – The where and When of the crime. Opportunities usually arise when certain vulnerabilities or weaknesses are present. **Means** – Pertains to the capabilities a criminal would need to be successful.
Salami Attack	Committing several small crimes with the hope that the overall larger crime will go unnoticed. • Most common example involves subtracting a small amount of funds from several accounts with the hope that such an insignificant amount would be overlooked.
Script Kiddies	Hackers that do not necessarily have the skill to carry out specific attacks w/out the tools are provided for them on the Internet and through friends.
Data Diddling	Refers to alteration of existing data. Many times this occurs before it is entered into an application or as soon as it completes processing and is outputted from an app. • Usually done is to overstate revenue and assets and understate expenses and liabilities • Very common and easiest to prevent by using access and accounting controls, supervision, separation of duties and authorization limits.
Excessive Privileges	When a user has more computer rights, permissions and privileges than what is required for the tasks they needs to fulfill • **Authorization Creep** – when a person slowly gains more access to different parts of the process. I.e. moved from one dept to another, but rights were not removed from the other department.
Password Sniffing	Sniffing network traffic with the hope of capturing passwords being sent b/t computers
IP Spoofing	Manually change their IP address or use a tool to do this for them. Considered a masquerading attack. • Using IPv6 or IPv4 using IPSec can be used to help fight IP spoofing, but for this to be successful everyone would need to use this technology.
Denial of Service	A general term for many different types of attacks. Goal is denying others the service that the victim system usually provides. • Types are SYN attacks, Ping of Death, fragment attacks, and DDOS attacks. **DoS vs. DDoS** **DoS** – is usually one computer attacking the availability of another system **DDoS** – is using a number of computers to attack the availability of another system.
Dumpster Diving	Rummaging through a companies or individual's garbage for discarded documents, info, and other items that could be used in an attack against the person or company. • Is unethical, but legal unless done by trespassing on someone else's property.
Due Care	Means a company did all that it could have reasonable done to try and prevent security breaches, and also took necessary steps to ensure that if a security breach did take place, damages were reduced b/c of the controls or countermeasures that existed. • A company practiced common sense and prudent mgmt practices with responsible actions.
Due Diligence	Means that the company properly investigated all of their possible weaknesses and vulnerabilities before carrying out any due care practices. • Due diligence is about researching and assessing the current level of vulnerabilities so that the true risk level is understood
Prudent Person Rule	Mgmt must follow, which requires mgmt to perform duties that prudent and responsible people would exercise in similar circumstances.
Agreements with other	• When companies come together to work in an integrated manner, such as extranets and VANS,

companies	special care must be taken to ensure that each party promises to provide the necessary level of protection, liability, and responsibility needed, which should be in the contracts • **Downstream liability** – Both companies need to make sure that they are doing their part to ensure that their activities, or lack there of, will not negatively affect another company. • **Responsibility** – refers to the obligation and expected actions/behaviors of a particular party • **Obligation** – can have a defined set of specific actions required • **Accountability** – the ability to hold a party responsibility for certain actions or inactions
Legal Recognized Obligation & Proximate Causation	For negligence to be proven in court, there usually needs to be a **legally recognized obligation**, which means there is a standard of conduct expected of the company to protect others from unreasonable risk. • There must also be **Proximate Causation** – meaning someone can prove that the damage that was caused was the company's fault. **Examples** **Legally recognized obligation:** • Cheapo Inc, did not effectively protect customers' assets **Failure to conform to the required standard:** • By not erecting the proper security policy and program they broke 12 federal regulations **Proximate Causation and resulting injury or damage:** • Fact that 22 individuals lost money was directly related to the financial institutions lack of implementing basic requirements and not practicing due care.
3 Types of Laws	1. **Civil Law** 2. **Criminal Law** 3. **Administrative/Regulatory Law**
Civil Law	**AKA Tort** – deals with wrongs against individuals or companies that result in damage or loss. • Would result in a financial restitution and/or community service instead of jail. • If someone took another person to a civil court, the jury would decide upon liability instead of innocence or guilt. • If the person was found liable then the jury would decide upon punitive damges • Brought by the wronged party instead of a criminal case, which would be the government. • **Petitioner** – person who brings the lawsuit • **Respondent** – person the lawsuit was filed against. • Burden of proof is on the respondent. • Level of proof is lower • Dedicision is made based on **Preponderance of the Evidence** – means the winning party is the one whose story the judge or jury believes. **Monetary damages awarded types:** 1. **Compensatory damages** – Actual amount of loss suffered or expected to. 2. **Pain and Suffering** – compensation for mental anguish and psychological damage 3. **Punitive Damages** – above and beyond the petitioner losses. Meant to deter you and others from repeat issue
Administrative/Regulatory Law	Deals with regulatory standards that regulate performance and conduct. Government agencies create these standards. • Held according to court procedures but are before councils or judges that are not officers of the court
Criminal Law	Used when an individuals conduct violates the government laws which have been developed to protect the public. Jail sentences are usually the punishment. • **Complainant** – person that files the complaint • **Defendant** – person or organizations against whom the charges are filed. • Burden of proof is on the government. **Penalties for violation:** 1. **Montary payment** 2. **Loss of liberty (jail)** 3. **Restriction of liberty (probation)** **Types of criminal violations:** 1. **Felonies** – Most serious offenses. Jail or death 2. **Misdemeanors** – Less serious can be sentenced to jail fo fined 3. **Violations** – only be fined
3 ways laws originate	1. Through legislation (statutory law) 2. Court Decisions (case law) 3. Common practice and usage (common law)
Trade Secret	Protects certain types of info or resources from unauthorized use or disclosure. For it to qualify for a

	trade secret the resource must provide the company with some type of competitive value or advantage. • Something that is proprietary to that company and important for its survival and profitability. • I.e. formula for coke
Copyright	Protects the right of an author to control the public distribution, reproduction, display, and adaptation of his original work. • Covers pictorial, graphic, musical, dramatic, literary, motion pictures, sculptural, sound recording, and architectural. • It protects the expression of the idea of the resources instead of the resource itself. • Computer programs and manuals are examples cover under Federal Copyright act
Trademark	Used to protect a word, name, symbol, sound, shape, color, or combo of these.
Patent	Given to individuals or companies to grant the owner legal ownership and enable the owner to exclude others from using or copying the invention. • Invention must be novel, useful, and not obvious • Grants a limited property right to exclude others from making, using, or selling the invention for a specific period of time. • Protects the idea itself
Internal protection of intellectual property	• Intellectual property protected by the previously mentioned laws need to be identified and integrated into the company's data classification scheme. • Resources should have the necessary level of access control protection, auditing enabled, and proper storage environment. • If a company fails in one or all of these steps, they may not be covered by the laws b/c they did not practice due care.
Software Piracy Organizations	1. **SPA** – SW Protection Association – formed by major companies to enforce proprietary SW rights. 2. **FAST** – Federation Against SW Theft – Headquartered in London, provide similar functionality as SPA but Internationally 3. **BSA** – Business SW Alliance – based in DC, provide similar functionality as SPA but Internationally • One of the offenses is decompiling vendor object code to reverse engineer it in hopes of understanding its functionality or security flaws. • **DMCA** – Digital Millennium Copyright Act – makes it illegal to create products that circumvent copyright protection mechanisms
Chain of Custody	Dictates that all evidence be labeled with info indicating who secured and validated it. • A history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. • B/c electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.
Incident Handling	Clearly defined incident handling process can be more cost effective, enable recovery to happen more quickly, and provide a uniform approach with certain expectation of its results. • Should be part of the DR plan • Primary goal is to contain and repair any damage caused by an event and to prevent any further damage. • Should also be closely linked to security training • Employees should know how to report an incident to the incident handling team. • Process should be centralized, easy to accomplish, convenient, and welcomed.
Hearsay	Evidence is secondhand evidence. Computer related documents are considered hearsay • Not admissible in court unless it has firsthand evidence that can be used to prove the evidence's accuracy, trustworthiness, and reliability, such as a businessperson who generated the computer logs and collected them. • Important that the person generates and collects logs as a normal course of business, not just for the court.
Lifecycle of evidence	1. Collection and identification 2. Storage, preservation, and transportation 3. Presentation in court 4. Being returned to victim or owner.
Best Evidence	Primary evidence used in a trial b/c I provides the most reliability. • Example is an original signed contract • Oral evidence is not considered best evidence b/c there is no firsthand reliable proof that supports its validity.
Secondary Evidence	Not viewed as reliable and strong in proving innocence or guilt when compared to best evidence. • Oral evidence, such as a witness testimony, and copies of original documents

Direct Evidence	Prove a fact all by itself instead of needing backup info to refer to. Presumptions are not required. • Many times direct evidence is based on info gathered from a witness's five senses
Conclusive Evidence	Irrefutable and cannot be contradicted. Strong by itself and does not require corroboration
Circumstantial Evidence	Prove an immediate fact that can then be used to deduce or assume the existence of another fact. • Used so that the judge or jury will logically assume the existence of a primary fact.
Corroborative Evidence	Supporting evidence used to help prove an idea or point. • Cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.
Opinion Evidence	When a witness testifies, the **opinion rule** dictates that they must testify to only the facts of the issue and not there opinion of the facts. • Slightly different from an expert witness b/c there are used primarily for his educated opinion
Hearsay Evidence	Oral or written evidence presented in court that is secondhand and that has no firsthand proof of accuracy or reliability.
Evidence	Evidence must be **sufficient, reliable, and relevant** to the case 1. **Sufficient** – must be persuasive enough to convince a reasonable person of the validity of the findings 2. **Reliable** – must be consistent with the facts. Factual not circumstantial 3. **Relevant** – must have reasonable and sensible relationship to the findings. **If a piece of evidence is found to be sufficient, reliable, and relevant, it must also be legally permissible** – meaning it was obtained in a legal way.
Surveillance	**2 main types pertaining to computer crimes:** 1. **Physical** – pertains to security cameras, security guards, CCTV, and undercover agent. 2. **Via the computer** – auditing events which passively monitors events by using network sniffers, keyboard monitors, wiretaps, and line monitoring. • In most jurisdictions active monitoring requires a search warrant. • Fourth amendment protects US citizens from unlawful search and seizure from law enforcement. But private citizens are not subjected to protecting the 4th amendment rights of others unless they acting as police agents.
Exigent Circumstances	If a law enforcement agent seizes evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence.
Enticement and Entrapment	**Enticement** – is luring an intruder and is legal and ethical **Entrapment** – induces a crime, tricks a person, and is illegal.
Import and Export Laws	In the US the Bureau of Export Admin (BXA) governs exportation of encryption mechanisms
Privacy	Federal Privacy Act was put in place to protect US citizens sensitive info. • States that any data collected must be done in a fair and lawful manner • Data is only to be used for the purposes it was collected for • Held for a reasonable amount of time • If an agency collects data about a person, that person has the right to receive a report outlining data collected about them • Monitoring must be work related • Monitoring must also occur in a consistent way where all employees are subject to monitoring instead of picking out one or 2 people
HIPAA	Health Insurance Privacy and Accountability Act – provides national standards and procedures for the storage, use, and transmission of personal medical info and health care data
GLBA	Requires financial institutions to develop privacy notices and give their customers the option to prohibit the banks from sharing their info with nonaffiliated third parties. • Dictates that the board of directors is responsible for many of the security issues w/in a financial institution, indicates that risk mgmt must be implemented.
Computer Fraud and Abuse Act	Primary federal antihacking statute. Categorizes 7 forms of activity as federal crimes
Federal Privacy Act of 1974	Requires the following stipulations • Disclosure of personal info is limited to only authorized persons • Records must be accurate, relevant, timely, and complete • Safeguards are required to ensure security and confidentiality of records
European Union Principals on Privacy	Addressing using and transmitting data considered sensitive in nature. Six principals: 1. Reason for gathering of data must be specified at time of collection 2. Data cannot be used for other purposes 3. Unnecessary data should not be collected 4. Data should only be kept for as long as it is needed to accomplish the stated task 5. Only the necessary individuals who are required to accomplish the task should be allowed to access

	the data 6. Secure storage of the data and not allow unintentional leaking of data.
Computer Security Act of 1987	Requires federal agencies to identify computer systems that will contain sensitive info and the agency must develop security policy and plan for each of these systems
Security and Freedom through Encryption Act	Guarantees the right of all US citizens and residents to be able to use and sell encryption products and technology. • Also prohibits stat and federal governments from requiring anyone to relinquish encryption keys
Federal Sentencing Guidelines	Provide judges with courses of action to take when overseeing white collar crimes that take place within organizations • Guidelines provided ways in which companies and law enforcement should prevent, detect, and report computer crimes.
Economic Espionage Act of 1996	Enables the FBI to investigate industrial and corporate espionage cases.
Other Items	• Wiretapping is a passive attach that eavesdrops on communication. Only legal with prior consent or a warrant • Trademarks are items that are used to distinguish products form the competitors products • If companies are going to use any type of monitoring, they need to make sure it is legal in there area and inform all employees that they may be subjected to monitoring. • Logon banners should be used to inform users of what could happen if the do not follow the rules pertaining to using company resources. Provides legal protection for the company • Three main types of harm addressed in computer crime laws pertain to unauthorized intrusion, unauthorized alteration or destruction, and malicious code. • Law enforcement and the courts have a hard time with computer crimes b/c of the newness of the types of crimes, complexity involved, jurisdiction issues, and evidence collection. New laws are being written to properly deal with cybercrime. • Elements of negligence include not fulfilling a legally recognized obligation, failure to conform to a standard, and proximate causation, which result in injury or damage • Most computer crimes are not reported b/c the victims are not aware of the crime or are too embarrassed to let anyone else know. • Theft is no longer restricted to physical constraints. Assets are now viewed as intangible objects that can also be stolen or disclosed via technology means. • Companies should develop their own incident response team, which is made up of people from mgmt, IT, legal, HR, public relations, and security and other key areas of the organization. • To be admissible in court, business records have to be made and collected in the normal methods of business, not specially generated for a case in court. Business records can easily be hearsay if there is no firsthand proof of their accuracy and reliability. • Blue boxing simulates a tone that tricks the phone company's system into thinking the user is authorized for long distance service, which enables him to make the call for free • Red Boxing simulates the sound of coins being dropped into a pay phone • Black boxing manipulates the line voltage to receive a tool free call. • After a computer system is seized, the investigators should make a bit mirror image copy of the storage media before doing anything else

9. Application and System Development

Topic	Description
SW's Importance	• Security should be interwoven into the core of a product and provide different layers • Application system controls can control input, processing, number-crunching methods, interprocess communication, interfacing to the system and other programs, access, and output • Controls can be preventative, detective, or corrective
Device vs. SW Security	Division b/t SW security and device security deals with providing security at the beginning stages of SW development vs. providing devices that protect the perimeters of networks

	Perimeter devices are more often considered that SW development b/c: 1. In the past, it was not crucial to implement security during the SW development stages; thus, programmers do not practice these procedures 2. Many security professionals are not SW developers 3. Many SW developers do not have security as a main focus 4. SW vendors are trying to rush their products to market with their eyes set on functionality not security 5. Computing community is used to receiving SW with bugs and applying patches 6. A combo of the preceding.
Environment vs. Application Controls	SW controls can be implemented by the OS, application or through DB mgmt controls, and usually a combo of all 3.
Complexity of functionality	Programmers and application architects need to find a happy medium b/t necessary functionality of the program, security requirements, and the mechanisms that should be implemented to provide security.
Data types, format and length	• Buffer overflows are caused by the program not making sure that only the right amount of info is accepted. • Data also needs to be in the right format and data type and be reasonable so they are not passed to calculations and logic procedures
Implementation and default issues	• When a security application or device is installed, it should default to NO ACCESS. • Fine line b/t user friendliness, functionality, and security • If an application is userfriendly, it is probably not secure because if requires a lot of extra coding. • Implementation errors and misconfigurations are common issues that cause a majority of security issues in network environments.
Failure States	• If an app fails it should return to a safe and more secure state • If an app fails and is executing in privileged state, these processes should be shut down properly and released to ensure that disrupting a system could not provide compromises that could be expoited.
DB Mgmt	**DBMS** – usually a suite of programs used to manage large sets of structured data with ad hoc query capabilities for many types of users **Database** – a collection of data stored in a meaningful way that enables multiple users and applications to access, view, and modify data as needed. • DB is the mechanism that provides structure for data that is collected.
DB Jargon	**Record** – collection of related data items **File** – Collection of records of the same type **DB** – cross-referenced collection of files **DBMS** – Manages and controls the DB **Base Relation** – A table stored in a DB **Tuple** – a row in a 2 dimensional DB **Attribute** – A column in a 2 dimensional DB **Primary Key** – Columns that make each row unique (table must include a primary key for every row) **View** – Virtual relation defined b the DB to keep subjects from viewing certain data **Foreign Key** – Attribute of one tale that is the primary key of another table **Cell** – Intersection of a row and column **Schema** – Holds data that describes a DB **Data Dictionary** – Central repository of data elements and their relationships.
DB Models	Defines the relationships b/t different data elements, dictates how data can be accessed, and defines acceptable operations, type of integrity offered, and how the data is organized.
Relational DB model	Uses attributes (columns) and tuples (rows) to contain and organize info. • Most widely used model • Present info in the form of tables • Composed of 2 dimensional tables, and each table contains unique rows, columns, and cells. • Primary key is a field that links all the data w/in a record to corresponding value. • An app uses its procedures to obtain data from the DB. DB does not actually provide procedures
Hierarchical DB model	Combines records and fields that are related in a logical tree structure. • Parents have 1 child, many children, or no children • Tree structure contains branches, and each branch has a number of leaves, or data fields • Useful for mapping one to many relationships
Distributed DB model	Has data stored in more than one DB, but it is logically connected. • Model enables different DB to be managed by different admins. • May be useful if each DB contains info that is specialized, but the complexity of load

	balancing, fault tolerance, and shifting of users is quite high
Object-oriented DB	Designed to handle a variety of data. Objects w/in the DB contain info that is used to access the objects actually containing these different data types and defines their properties. • More dynamic in nature when compared to a relational DB b/c objects can be created when needed, and the data and procedure go with the object when it is requested • Has classe • s to define the attributes and procedures of its objects • Can be used to dynamically build different web pages for different users depending upon their requests and input to a particular web site. • The objects are used to build the page, and the procedures w/in the objects dictate how the data w/in the objects will actually be used to perform their tasks.
DB Interface Languages	1. **ODBC** – Open DB Connectivity – An API (App Programming Interface) that allows an app to communicate with a DB either locally or remotely. • The app sends requests to the ODBC, which in turn translates then into DB commands • ODBC tracks down the necessary DB driver for the app 2. **OLE DB** – Object Linking and Embedding – Separates data into components that run as middleware on a client or server • Provides low level interface to link info across different DB and provides access to data no matter where it is located or how it is formatted. 3. **ADO** – ActiveX Data Objects – An API that allows applications to access back end DB systems. • Set of ODBC interfaces that expose the functionality of a DB through accessible objects • ADO uses the OLE DB interface to connect w/ the DB and can be developed with many different scripting languages. 4. **JDBC** – Java DB Connectivity – An API that allows a java application to communicate with a DB. • App can connect through ODBC or directly to the DB 5. **XML** – Extensible Markup Language – A standard for structuring data so that it can be easily shared by apps using web technologies. • A markup language that is self defining and provides a lot of functionality in how info w/in the DB is presented • Web browser interprets the XML Tags
Core Functionalities of DB	1. **DDL** – Data Definition Language – Defines the structure and schema of the DB. • Structure defines table size, key placement, and data element relationship • Schema describes the type of data that will be held and manipulated and its properties. Defines the structure of the DB, access operations, and integrity procedures 2. **DML** – Data manipulation Language – Examines and manipulates the data w/in a DB • Contains all the commands that enable a user to view, manipulate, and use the DB (view, add, modify, sort, and delete commands) 3. **QL** – Query Language – users to make queries and access the data w/in the DB 4. **Report Generator**
Data Dictionary	A central repository of data elements and their relationships. • Stores critical info about data usage, data relationships, data sources, and data formats. • A tool used to centrally manage parts of a DB by controlling data about the data (referred to as **Metadata**) with in DB. • Central collection of data element definitions, schema objects, and reference keys • Contains the default values for columns, integrity info, the names of users, the privileges and roles for users, and auditing info. • DBMS reads the data dictionary to ascertain that schema objects exist and checks to see if specific users have the process access rights to view them • Users specific views are stored in the data dictionary.
Primary vs. Foreign key	**Primary key** – is an identifier of a row and it must be unique. Each row must have a primary key **Foreign key** – if an attribute in one table has a value matching the primary key in another table, this attribute is considered a foreign key. • Foreign key is not necessarily the primary key in its current table; it only has to contain the same info that is held in another tables primary key.
Integrity	**Concurrency** – has to do with making sure that different subjects receive the most up to date info and ensures that the DB can properly handle various requests at the same time. • If controls are not in place, 2 users can access and modify the dame data at the same time

	• To ensure that concurrency problems do not exist, processes can **lock** tables w/in a DB, make changes, and then release the SW lock. • Locking ensures that 2 processes do not access the same table at the same time. **DB SW 3 types of Integrity Services:** 1. **Semantic Integrity** – Mechanisms makes sure that structural and semantic rules are enforced. These rules pertain to data types, logical values, uniqueness constraints, and operations that could adversely affect the structure of the DB 2. **Referential Integrity** – If all foreign keys reference existing primary keys. 3. **Entity Integrity** – guarantees that the tuples are uniquely identified by primary key values. • Every tuple must contain one primary key, if it doesn't it cannot be referenced by the DB.
Operations that protect integrity of the Data w/in a DB	1. **Rollbacks** – a statement that ends a current transaction and cancels all other changes to the DB. • Changes could have taken place with the data itself or with schema changes that were typed in. • When it is execute the changes are cancelled and DB returns to its previous state. 2. **Commit** – a statement terminates a transaction and executes all changes that were just made by the user. • Once the commit command is executed the changes are committed and reflected in the DB • By committing these changes, they are now available to all apps and users. • If a user attempts to commit a change and it cannot complete correctly, a rollback is performed. Ensures that partial changes do not take place and that data is not corrupted. 3. **Savepoints** – used to make sure that if a system failure occurs, or if an error is detected, the DB can attempt to return to point before the system crashed or hiccupped. • Are easy to implement win DB, but a balance has to b struck b/t too many and not enough • Having to many savepoints can degrade performance of the DB. • Not having enough runs the risk of loosing data and decreasing user productivity. • Can be initiated by a time interval, specific action by the user, or the number of transactions or changes made to the DB. 4. **Checkpoints** – similar to save points. When a DB SW fills up a certain amt. Of memory a checkpoint is initiated, which saves the data from the memory segment to a temp file.
DB Security Issues: Aggregation and Inference	**Aggregation** – happens when a user does not have the clearance or permission to access specific info, but does have the permission to access components of this info. • Act of combining info from separate sources and the comb forms new info, which the subject does not have the necessary rights to access. Combined info has a sensitivity that is greater than the individual parts. **To prevent Aggregation:** • The subject, and any application or process acting on the subjects behalf, needs to be prevented from gaining access to the whole collection, including the independent components. • Objects can be placed into containers, which are classified at higher levels to prevent access from subjects w/ lower level permissions or clearances. • Subjects queries can also be tracked and context-dependent access control be enforced (restricts access attempts if there is an indication of an aggregation attack. **Inference** – happens when a subject deduces or figures out the full story from the pieces they learned of through aggregation. **To prevent Inference:** • Implement **content – and context-dependent** access control rules that track the subjects query requests and restrict patters that represent inference. • **Cell Suppression** – a technique used to hide or not show specific cells that contain info that could be used in inference attacks • **Partitioning** – a DB involves dividing the DB into different parts, which makes it marder fo an unauthorized individual to find connecting pieces of data that can be brought together and other info that can be deduced or uncovered. • **Noise and pertubation** – Technique of inserting bogus info in the hopes of misdirecting an attacker of confusing the matter enough that the actual attack is not fruitful. • OS security is based on the identity and authentication of the subject. Makes decisions based about whether a subject can access a file, not based on contents of file.

	• DB security looks at the contents of a file when making access control decision and is called **Content-based Access Control –** type of access control increases processing overhead, but provides higher granular control.
DB views	Databases can permit one group, or a specific user, to see info. • Like OS DB can employe DAC and MAC controls. • Views can be displayed according to group membership, user rights, or security labels. • If DAC employed then groups and users could be granted access through view based on identity, authentication, and authorization. • If MAC were in place, then groups and users would be granted access based on their security clearance and the data's classification level.
Polyinstantiation	Deals with not allowing users at one level to access and modify data at a higher level. • Enables a relation to contain multiple tuples with the same primary keys, with each instance distinguished by a security level. • When this info is inserted into a DB, lower level subjects need to be restricted from it. • Instead of restricting access, another set of data is created to fool the lower-level subjects into thinking that info actually means something else. • Used to prevent inference attacks • Whenever a copy of an object is created and populated with different data, meaning 2 instances of the same subject have different attributes, polyinstantiation is in place.
OLTP	**Online Transaction Processing –** usually used when DB are clustered to provide fault tolerance and higher performance. • Provides mechanisms that watch for problems and that deal with them appropriately when they do occur. • Any erroneous or invalid transactions that are detected should be written to a transaction log and to a report log to be reviewed at a later time. • Will load balance incoming requests if it is necessary. This means that if requests to update DB increase, and one system reduces in performance b/c the large volume, OLTP can move some of these request to other systems • **2 phase commit service** – OLTP will make sure that a transaction is not complete until all DB receive and reflect the change. • OLTP records transactions in real time, which updates more than one DB in a distributed environement. This type of complexity can introduce many integrity threats, so the DB SW should implement the characteristics of the **ACID test**; **ACID Test Characteristics**: 1. **Atomicity** – Divides transactions into units of work and ensures that all modifications take effect or none take effect. Changes are either committed or the DB is rolled back. 2. **Consistency** – A transaction must follow the integrity policy developed for that particular DB and ensure that all data is consistent in the different DB. 3. **Isolation** – Transactions execute in isolation until completed, w/out interacting with other transactions. The results of the modification are not available until the transaction is completed. 4. **Durability** – Once the transaction is verified as accurate on all systems, it is committed, and the DB is not rolled back
Data Warehousing and Data Mining.	**Data Warehousing** – combines data from multiple DB or data sources into a large DB with the purpose of a fuller extent of info retrieval and data analysis. • Enables users to query one entity rather than accessing and querying different DBs. • Method of selecting useful info that is then processed and presented in a more useful and understandable way. • Instead of having every piece of data presented, user is given data in a more abridged form that best fits the users needs. • Because the warehouse is in one place it requires more stringent security. **Data Mining** – process of massaging the data held in the data warehouse into more useful info • Data mining tools are used to find an association and correlation in data to produce **metadata**. • Metadata can show previously unseen relationships b/t individual subsets of info. • Can look at complex data and simplify it by using Fuzzy logic, a set theory, and expert systems to perform the mathematical functions and look for patterns in data that are not so apparent • Data goes into a DB and metadata comes out of the DB • Data mining is also known as **KDD** (**Knowledge Discovery in DB)** and is a combo of techniques to identify valid and useful patterns **3 approaches KDD systems uncover patterns**

	1. **Classification** – Data is grouped together according to shared similarities 2. **Probabilistic** – Data interdependencies are identified and probabilities are applied to their relationships 3. **Statistical** – Identifies relationships b/t data elements and uses rule discovery.
Mgmt of Development	• A security plan should be drawn up at the beginning of a development project and integrated into the functional plan to ensure that security is not overlooked • First plan is broad, covers a wide base, and refers to documented references • Security plan should have a lifetime of its own. It will need to be added to, subtracted from, and explained in more detail as the project continues.
Life Cycle Phases	1. Project initiation 2. Functional design analysis and planning 3. System design specifications 4. SW development 5. Installation/implementation 6. Operational/maintenance 7. Disposal **Security should be embedded through all phases.**
Project Initiation	• The characteristics of the system and proposed functionality are discussed, brainstorming sessions take place, and obvious restrictions are reviewed. • Conceptual definition of the project needs to be initiated and developed • Phase include evaluating products that are currently on the market and could identify any demands that are not being met by current vendors. • High-level proposal should be drafted that outlines the necessary resources for the project, predicted timeline for development, and projected profit • User needs are defined and basic security objectives of the product. • Determine if product is processing sensitive data or not and levels of sensitivity should be defined. • Initial risk analysis should be initiated that evaluates threats and vulnerabilities to estimate the cost/benefit ratios of the different security countermeasures. • Issues pertaining to security integrity, confidentiality, and availability need to be addressed. • Basic security framework is designed for the project to follow and risk mgmt processes are est.
Risk mgmt	• One of the most important pieces of risk mgmt is to know the right questions to ask. • First step in risk mgmt is to identify the threats and vulnerabilities and to calculate the level of risk involved. • When all risks are evaluated, mgmt will decide upon the acceptable level of risk • Compromises and intelligent business decisions need to be made to provide a balance b/t risk and economic feasibility.
Risk Analysis	• Performed to identify the relative risks and the potential consequences. • Once all risks are identified, the probability of them actually taking place needs to be quantified, and the consequences of these risks need to be properly evaluated to ensure that the right countermeasures are implemented w/in the development phase and the product itself. • Once threats are identified, probability of occurring is estimated, and their consequences are calculated, risks can be listed in order of importance. • These risks need to be addressed in the design and architecture of the product as well as in the functionality the product provides, the implementation procedures, and the required maintenance **Project risk analysis vs. Security risk analysis:** Project risk analysis – usually pertaining the risk of the project failing.
Functional Design Analysis and Planning	• A project plan is developed to define the security activities and to create security checkpoints to ensure that QA for security controls takes place and that the configuration and change control process is identified. • Security resources are identified, test schedules start to form, and evaluation criteria are developed to be able to properly test the security controls. • A formal functional baseline is formed, meaning the expectations of the product are outlines in a formal manner, usually through documentation. • Test plan is developed which will be updated throughout each phases. • Addresses the functionality required out of the product and is capture in design document • If the product is developed for a customer, the design document is used as a tool to explain to the customer what the developing team understands of the requirements of the product.
System Design Specifications	Software requirements come from Informational, functional, and behavioral models. 1. Informational model – dictates the type of info to be processed and how it will be processed 2. Functional model – outlines the tasks and functions that the application needs to carry out

	3. Behavioral model – explains the states that the application will be in during and after specific transitions take place. • Each state has to be accounted for to ensure that the product does not go into an insecure state and act in an unpredictable way • The informational, functional, and behavioral model data go into the SW design as requirements. • What comes out of the design is the data, architectural, and procedural design • Data design takes the informational model info and transforms it into data structures that will be required to implement the SW • The architectural design defines the relationships b/t the major structures and components of the application • Procedural design transforms structural components into descriptive procedures • This where **Access control mechanisms are chosen** • Subject rights and permissions are defined • Encryption method and algorithm are chosen • Handling of sensitive data is ironed out • Necessary objects and components are identified • Interprocessing communication is evaluated • Integrity mechanism is identified • Any other security specifications are appraised and solutions are determined • Work Breakdown Structure (WBS) for future phases needs to be confirmed, which includes the development and implementation stages. Includes a timeline and detailed activities for testing, development, staging, integration testing, and product delivery. • The system design tool used to describe the user requirements and the internal behavior of a system. It then maps the 2 elements to show how the internal behavior actually accomplishes the user requirements. • This phase addresses what mechanisms are needed to provide this functionality and determines how it will be coded, tested and implemented. • Testing needs to be taken under consideration and programmers can code in **hooks** that show the testers the state of the product at different stages of data processing
Software Development	• Phase where programmers and developers become deeply involved • This stage is where the programmers should code in a way that does not permit SW compromises • Debugging and code reviews should be carrier out by peer developers and everything clearly documented. • Formal and informal testing should begin and unit testing can start very early • Unit testing can be done by the programmer • Formal testing should be carried out by a totally different group – separation of duties. • SW hooks inserted for testing or modifications purposes need to be removed prior to being released. • Its important to map security risks to test cases and code. • Test should be conducted in an actual network, which should mirror the production environment to ensure the code does not only work in the labs • Security attacks and penetrations usually take place during this phase • Issues found in unit and formal testing are relayed to the development team in problem reports.
Verification vs. Validation	**Verification** – determines if the product accurately represents and meets the specifications. **Validation** – determines if the product provides the necessary solution for the intended real world problem. Main goal of the project is met.
Installation/Implementation	• Focuses on how to use and operate the developed system or application • At this phase the customer has purchased the product and installed it into their environment • Configurations should be documented and user guides and operation and maintenance manuals developed • Monitoring security activities needs to be performed to verify adhering to SLAs • Accreditation should occur b/t the implementation and beginning of the operational use of the system/app. • Certification was done by evaluating all security controls. • Accreditation looks at the whole system, not just the app.
Operational and Maintenance	• Configuration of the new system and validating security controls and conducting vulnerability tests, monitoring activities, and auditing events.
Disposal	When its time for a new app system the transition must happen in a secure manner

	• Info may need to be archived, backed up to another system, discarded, or destroyed
Postmortem Review	Method of looking at the project from an objective view and identifying issues that could be improved next time around.
System Life Cycle Phases	**1. Project initiation** • Conception of project definition • Proposal and initial study • Initial risk analysis **2. Functional design analysis and planning** • Requirements uncovered and defined • System environment specifications determined • Formal design created **3. System design specifications** • Functional design review • Functionally broken down • Detailed planning put into place • Code design **4. SW development** • Developing and programming SW **5. Installation/implementation** • Product installation and implementation • Testing and auditing **6. Maintenance support** • Product changes, fixes, and minor modifications **7. Disposal** • Replace product with new product
SW development Methods	1. **Waterfall** – Classical method that uses discrete phases of development that require formal reviews and documentation before moving into the next phase of the project. 2. **Spiral Model** – A method that builds upon the waterfall method with an emphasis on risk analysis, prototypes, and simulations at different phases of the development cycle. 3. **JAD** – Joint Analysis and Development – Uses a team approach in application development in a workshop oriented environment 4. **RAD** – Rapid App Development – A method of determining user requirements and developing systems quickly to satisfy immediate needs 5. **Cleanroom** – An approach that attempts to prevent errors of mistakes by following structured and formal methods of developing and testing. This approach is used for high quality and critical applications that will be put through a strict certification process.
Change Control	**Def** – a process to manage and approve of any type of change w/in the environment. • Changes must be authorized, tested, and recorded. Changed systems may require re-certification and re-accreditation. **Configuration mgmt** – procedures that are used to carry out changes that affect the network, individual systems or SW. • Identifying, controlling, accounting for and auditing changes made to the baseline TCB, which includes changes to HW, SW, and firmware • A system that will control changes and test documentation through the operational life cycle of a system
Capability Maturity Model	**CMM** – describes procedures, principals, and practices that underlie SW development process maturity. • Model was developed to help SW vendors improve their development process by providing an evolutionary path from ad-hoc approach to a more discipline approach • Aimed to improve SW quality, reduces the life cycle of development, provides better project mgmt capabilities, allows for milestones to be created and met in a timely manner • Goal is to continue to review and improve upon the processes to optimize output, increase capabilities, and provide higher quality SW at a lower cost. **5 maturity levels used:** 1. **Initial** – Development process is ad hoc or even chaotic. Company does not use effective mgmt procedures and plans. No assurance of consistency, and quality is unpredictable 2. **Repeatable** – A formal mgmt structure, change control, and QA in place. Company can properly repeat processes throughout each project. Formal process models defined 3. **Defined** – Formal procedures are in place that outline and define processes that are carried out in each project. Org has a way to allow for quantitative process improvement 4. **Managed** – Company has formal processes in place to collect and analyze qualitative data,

	and metrics are defined and fed into the process improvement program 5. **Optimizing** – The company has budgeted and integrated plans for continuous process improvement
SW Escrow	A third part will keep a copy of the source code and possible other materials, which will only be released to the customer if specific circumstances arise. Mainly if the SW vendor goes out of business.
Machine Language	In a form that the processor can understand and work with directly
Assembly and high-level languages	Cannot be understood directly by the processor and must be translated , which results in machine language.
Compiler	Function is to turn human understandable programming language into machine understandable language or object code. • Translate large sections of code at a time • Most applications are compiled
Interpreters	Translate one command at a time to object code at time of execution • Many scripting languages are interpreted
Assemblers	Translate assembly language into machine language.
Object Oriented Concepts	**Object Oriented Programming (OOP)** – works with classes and objects. A real world object is a member (or instance) of a larger class of objects. The class can have a set of attributes associated with it, and when an object is generated, it inherits these attributes • Once the class is defined, the attributes can be reused for each new member or instance of the class that is created. • **A Method** – is the functionality or procedure that an object can carry out (i.e. accept data from a users and reformat). • Objects are unique instances of a data structure defined by the template provided by their corresponding classes. • Objects communicate to each other by using **messaging** • Message is made up of the destination, the method that needs to be performed, and corresponding arguments. • An object can have a shared portion and a private portion, • Shared portion is the interface that enables the object to interact with other components. Messages enter through the interface to specify the requested operation or method to be performed. • Private part of an object can be how it actually works and performs the requested operations, this is a form of Info hiding. • Data hiding is provided by encapsulation, which protects an objects private data from outside access. • Once the objects are defined, it is necessary to develop a classification structure which means that instances of an object are defined and named. • Structure to the classification defines the necessary relationships b/t the objects. Structure representation is a way of partitioning the requirement of the model. • Messaging can happen in several ways. 2 objects can have a single connection (one-to-one), a multiple connection (one-to-many) and a mandatory connection or an optional connection. • Its important to map the messaging communication paths to identify if info can flow in a way that is not intended. Help ensure that sensitive data cannot be passed to objects of a lower security level. • Each object can be reused which enables more efficient use of resources and programmers time. • Different apps can use the same objects so there is a reduction in redundant work and as an application grows in functionality, objects can be easily added and integrated into the original structure. • Objects can be catalogued in a library, which provides an economical way for more than 1 app to call upon the objects. • **Object oriented method is a modular approach** and slows components to be reused, complexity is reduced, and parallel development can be done. These characteristics allow for fewer mistakes, easier modification, resource efficiency, and more timely coding than the classics information flow models • **OOP also provided functional independence** which means that each module addresses a specific subfunction of requirements and has an interface that is easily understood by other parts of the app. • Object is encapsulated meaning that the data structure (the operational functionality) and the acceptable ways of accessing are grouped into one entity.

	• **OOD**- Object Oriented Design – creates a representation of a real-world problem and maps it to a SW solution. System is modeled as a collection of cooperating objects. Each individual object is treated as an instance of a class w/in a class hierarchy • Design interconnects data objects and processing operations. • This programming approach is different from others b/c it allows for abstraction, modularity, and info hiding • Modularity is accomplished by using objects, applets, and agents
Polymorphism	Means that an object's response to a message is determined by the class to which the object belongs. • When different objects respond to the same command, input, or message in different ways. • I.e. 3 objects receive the input Bob. Object A would process the input and output 43 years old. Object B would receive the input and produce the output Husband of Sally.
OOA	**Object Oriented Analysis** – process of classifying objects that will be appropriate for a solution. A problem is analyzed to determine the classes of objects to be used in an application.
OOP	**Object Oriented Programming** – is a class of programming languages and techniques that are based on the concepts of objects and a set of routines and methods, which operate on the data
Structured Analysis Approach	Looks at all objects and subjects on an app and maps their interrelationships, communication paths and inheritance properties, which was indicated above. • OOA is an example
Data Modeling	Considers data independently of the way that the data is processed and of the components that process the data. A data model will follow an input value from beginning to end an verify that the output is correct. • Looks specifically at the output • Data modeling verify that pointers are actually pointing to the right place
SW Architecture	• An architectural view looks at how the app actually meets and fulfills the requirements recognized and agreed upon in the design phase. • SW architecture will break requirements into individual units that need to be achieved by functionality w/in the app. • This way of developing a product provides more control and modularity of issues and solutions. • Software Architects need to provide a high-level view of all app objectives and vision of the overall project goals.
Data Structure	A representation of the logical relationships b/t elements of data. • Dictates the degree of association b/t elements, methods of access, processing alternative, and the org of data elements
Cohesion and Coupling	**Cohesion** – a module that can perform a single task with little or no help from other modules. Does just one function. • The more a module can do on its own the better, b/c requiring a lot of interaction b/t modules makes it harder to modify one module down the road w/out affecting other modules. **Coupling** – is a measure of interconnection among modules in an app. • The lower the coupling the better the SW design, b/c it promotes module independence. More independent a component is, the less complex the app is and the easier it is to modify and troubleshoot. • Modules should be self-contained and perform a single logical function, which is cohesion. Modules should not drastically affect each other, which is low coupling.
ORBs and COBRAs	The Object Mgmt Architecture (OMA) provides standards to accomplish a complete distributed environement. It contains 2 main parts: 1. System oriented components – **Object Request Brokers (ORBs)** and object services 2. Application-oriented components (application objects and facilities). **ORB** – manages all communication b/t components and enables them to interact in a heterogeneous and distributed environment. • ORB works independently of the platforms where the objects reside, which provides greater interoperability. • ORB relies on object services to provide access control. Track relocated objects, and create objects • ORB is the middleware that est. the client/server relationship b/t objects. • When a client needs to access an object on a server the ORB intercepts the request and is responsible for finding the object. • Once the object is found, ORB invokes an operation, passes the parameters, and returns the results to the client. • When objects communicate to each other they use pipes, communciaition services. ORB is a pipe. • ORBs provide communication b/t distributed objects

	• ORBs are mechanisms that enable objects to communicate locally or remotely **COBRA – Common Object Request Broker Architecture** – provides interoperability among th vast array of SW, platforms, and HW in environments. • Enables applications to communicate with one another no matter where the application is located or who developed it.
CASE	**Computer Aided SW Engineering** – a general term for tools that help make program applications more quickly and with fewer errors in an automated fashion. • First CASE tools were translators, compilers, assemblers, linkers, and loaders • Graduated to program editors, debuggers, code analyzers, and version control mechanisms. • CASE applies engineering principals to the development and analysis of specifications using specific tools. • **Integrated-Computer Aided SW Engineering (I-CASE)** – When automation covers the complete life cycle of a product. • **CASE tools** – used for one specific part of the life cycle • **Rapid Prototyping** – more CASE tools utilize these technologies that enable applications to be developed faster with higher quality and lower cost. • A prototype can be made so that testing can begin earlier in the development process
Prototyping	Building a model of the gathered requirements of a SW product can show the customer where the development team is headed and its interpretation of the customers stated requirements. • Prototype also enables testing to being earlier in the development process so that errors or problems can be uncovered and addressed. • Security testing can also be done in earlier stages
COM and DCOM	**COM – Component Object Model** – defines how components interact and provides an architecture for simple interprocess communication (IPC) • Enables apps to use components on the same systems. **DCOM** – **Distributed Component Object Model** – Supports the same model for component interaction, but supports distributed IPC • DCOM enables applications to access objects that reside in different parts of the network • Has a library that takes care of session handling, synchronization, buffering, fault identification and handling, and data format translation • Acts as a middleware • DCOM provides ORB services, data connectivity services, distributed messaging services, and distributed transaction services layered over its RPC mechanism • DCOM uses the same interface as COM • Other types of middleware: • ORB • MOM – Message Oriented Middleware • RPC • ODBC
ODBC	A de facto standard that provides a standard SQL dialect that can be used to access many types of rational DB. ODBC is the middleman b/t apps and DBs.
OLE	**Object Linking and Embedding** – provides a way for objects to be shared on a local personal computer and to use COM as their foundation. • **Linking** – capability for one program to call another program. • **Embedding** – capability to place a piece of data inside a foreign program or document
DDE	**Dynamic Data Exchange** – enables apps to share data by providing IPC. Based on the client/server model and enables 2 programs or apps to send commands to each other directly
DCE	**Distributed Computing Environment** – Standard that was developed by the Open SW Foundation (OSF). It is basically middleware that is available to many venors to sue. • DCE provides an RPC servers, security service, directory service, time service, and distributed file support • DCE and DCOM provide the same functionality, but DCOM is Microsoft proprietary. • DCOM uses a **Globally Unique Identifier (GUID)** and DCE uses a **Universal Unique Identifier (UUID)** and are both used to uniquely identify users, resources, and components w/in an environment. • RPC function collects the arguments and commands from the sending program and prepares them for tansmission over the network. • RPC determines the network transport protocol that is to be used and finds the receiving host's address in the directory service
Enterprise Java Bean	**EJB** – A java component is called a java bean. A structural design for the development and implementation of distributed applications written in java. The EJC provides interfaces and methods

	to allow different applications to be able to communicate across a network environment.
Expert Systems and Knowledge based systems	**Expert Systems** are also called **knowledge-based systems** – use artificial intelligence to solve problems. • Expert system is a computer program containing a knowledge base and a set of algorithms and rules used to infer new facts from knowledge and incoming data. • AI SW uses nonnumerical algorithms to solve complex problems, recognize hidden patterns, prove theorems, play games, mine data, and help in forecasting and diagnosing a range of issues. • Expert systems emulate human logic to solve problems that would usually require human intelligence and intuition. • Expert system will attempt to think like a person, reason through different scenarios, and provide an answer even w/out the necessary data. • **Rule-based programming** – a common way of developing expert systems. Rules are based on if-then logic units that specifies a set of actions to be performed for a given situation • This is one way that expert systems are used to find patterns, which is called **pattern matching**. • A mechanism called the **inference engine**, automatically matches facts against patterns and determines which rules are applicable. An expert system consists of 2 parts: **1. Inference engine** – handles the user interface, external files, scheduling, and program-accessing capabilities. Used to decide how to execute a program or how the rules should be initiated and followed **2. Knowledge base** – contains data pertaining to a specific problem or domain. Provides the necessary rules for the system to take the original facts and combine them to form new facts. • Expert systems are built by a knowledge system builder (programmer), a knowledge engineer (analyst), and subject matter expert(s). • Commonly used to automate security log review for IDS • Use automatic logical processing, inference engine processing, and general methods of searching for problem solutions.
Artificial Neural Networks	An electronic model based on the neural structure of the brain. • Decisions by neural networks are only as good as the experiences they are given. • ANNs contain many units that stimulate neurons each with a small amount of memory. • Units work on data that is inputted through their many connections • Through training rules, the systems are able to learn from examples and have capability to generalize • In ANN, a connection b/t 2 units that is often activated might be strengthened, which is a form of learning. • The reason that some memories are more vivid than others is b/c more emotion is tied to them or more weight assigned. In ANN some inputs have higher weights assigned to them than other inputs, which amplifies the meaning or importance of the inputs . • Fuzzy logic an other mathematical disciplines are used for intuition, forecasting, and intelligent guessing. • ANN are programmed with the capability to decide and learn to improve their functionality through massive trial and error decision making
Java	An object oriented, platform independent programming language. Used to write full fledged pgrams and short programs, **applets**, which run on a user's browser. • Java is platform independent b/c it creates intermediate code, byte code, which is not processor specific an the Java Virtual Machine coverts the bytecode to the machine code.
Java Security	Java applets use a security scheme that employs a **Sandbox** to limit the applet's access to certain specific areas w/in the users system and protects the system from malicious or poorly written applets. • Applet is only supposed to run w/in the sandbox. • Sandbox restricts the applets environment by restricting access to a user's hard drives and system resources. • There is a different type of java applet, which is deemed **trusted** b/c it provides a digital signature. This type of applet has access to all system resources and is not confined to a sandbox. • This type is usually not a component on the Internet and is developed in-house and distributed w/in an intranet to provide some business-oriented functionality.
ActiveX	A Microsoft technology that is used to write controls that Internet users can download to increase their functionality and Internet experience. • Instead of trying to keep ActiveX components in a safe area for its computations and

	activities, this language practices security by informing the user where the program came from. • User can decide to trust this origin or not. • ActiveX technology provides security levels and authentication for users to be able to control the security of components they download • Unlike Java applets, ActiveX components are downloaded to a user's hard drive when he chooses to add the functionality that component provides. This means the ActiveX has far greater access to the user's system. • Relies on Authenticode technology that relies on digital certificates and trusting certificate authorities.
Malicious SW or Malware	Malicious code can be detected by the following: • File size increase • Many unexpected disk accesses • Change in update or modified timestamp • Sudden decrease of hard drive space • Unexpected storage activity by applications
Pseudo-flaw	Is code inserted into an app on purpose to trap potential intruders.
Virus	A small app, or string of code, that infects apps. • Main function of a virus is to reproduce and it requires a host app to be able to do this. • Viruses cannot replicate on their own. • Virus infects files by inserting or attaching a copy of itself to the file • When the infected program executes, the embedded virus is executed, which propagates the infection. • **Macro virus** – a virus written in on the macro languages (VB, Word basic) and is platform independent. They infect and replicate in templates and w/in documents. Macro viruses are common b/c the are easy to writ and office products are in wide use. • **Boot Sector Viruses** – viruses that infect the boot sector of a computer and either move data w/in the boot sector or overwrite the sector with new info • Some boot sector viruses have part of their code in the boot sector, which can intiate the virus and have the rest of the virues code in sectors on the hard drive it has marked off as bad. • **Compression Viruses** – viruses that append themselves to executable on the system and compress them using the users permission. • **Stealth Virus** – hides the modification that it has made to files or boot records. This can be accomplished by monitoring system functions used to read files or sectors and forging the results. • This means that when apps or users attempt to read and infected file or sector, the original, uninfected form will be presented instead of the actual infected form. • **Polymorphic Virus** – produces vaired but operational copies of itself. This is done in hopes of outwitting a virus scanner. Even if 2 copies are found and disabled, other copies may still remain active w/in the system. • Can use different encryption schemes requiring different decryption routines • These viruses can also vary the sequence of their instructions by including **noise** or bogus instructions, with other useful instructions • Also use a mutation engine and a random number generator to change the sequence of their instruction in the hopes of not being detected. • Has the ability of changing its own code, enabling the virus to have hundred or thousands of variants. • **Mutlipart virus** – infects both the boot sector of a hard drive and executable files. Virus first becomes resident in memory and then infects the boot sector. Once it is in memory, it can infect the entire system. • **Self-garbling virus** – attempts to hide from antivirus SW by garbling its own code. As the virus spreads it changes the way its code is formatted. A small portion of the virus code decodes the garbled code when activated. • **Meme viruses** – not actually viruses but types of e-mails that continually get forwarded around the Inet. Can be chain letters, email hoax virus alerts, religious messages. Replicated by humans and can waste bandwidth and spread fear • **EICAR test** – done with AV SW by introducing a benign virus to test the detection and reaction activities of the SW.
Worms	Can reproduce on their own w/out a host application and in that they are self contained programs. • Worm can propagate itself by using e-mail, TCP/IP and disk drives.

Logic bomb	Will execute a program, or string of code, when certain event happens or a data and time arrives.
Trojan Horse	A program that is disguised as another program. Trojan will perform the useful functionality of the imitated program in addition to the malicious functionality in the background • A host IDS can be configured to watch certain files and detect when they grow in size, which is often a sign of a Trojan • **Remote Access Trojans** – programs that run on systems and allow intruders to access the system remotely. They mimic functionality of legitimate remote control programs used for remote admin.
DoS	The network stack is the portion of the OS that enables devices to communicate over the network. Different OS and vendors interpret the RFCs for networking protocols differently, which end up in slightly different network stacks. • These differences can contain their own flaws that can be take advantage of to produces a DoS • DoS attacks can consume a victims bandwidth by flooding the network connection either from an attacker with more bandwidth than the victim or from several attackers • Another type of DoS attack can use up all the victims resources instead of consuming the networks bandwidth
Smurf	Type of DoS attack that uses ICMP Echo Requests. • Requires three players: the attacker, the victim, and the amplifying network. • The attacker spoofs or changes the source IP address in a packet header to make an ICMP Echo Request packet seem as though it originated at the victims system • The Echo Request message is broadcasted to the amplifying network which will reply to the victim with full force. • Causes the victims system to be overwhelmed and perhaps the victims network. **Countermeasures:** 1. To make sure a certain network is not used as an amplifying site, direct broadcast functionality can be disabled at border routers 2. Packets that contain internal source IP addresses should not be accepted by perimeter routers as incoming messages. 3. Only the necessary ICMP traffic should be allowed into and out of an environment. 4. A network IDS should be employed to watch for suspicious activity 5. Patches should be applied.
Fraggle	Similar to Smurf, but instead uses UDP as its weapon. Attacker broadcasts a spoofed UDP packet to the amplifying network, which in return replies to the victims system **Countermeasures:** 1. To make sure a certain network is not used as an amplifying site, direct broadcast functionality can be disabled at border routers 2. Packets that contain internal source IP addresses should not be accepted by perimeter routers as incoming messages. 3. Only the necessary ICMP traffic should be allowed into and out of an environment. 4. A network IDS should be employed to watch for suspicious activity 5. Patches should be applied.
SYN Flood	Continually sending the victim SYN messages with spoofed packets. • The victim will commit the necessary resources to set up this communication socket and it will send its SYN/ACK message waiting for a response but one will never come. • A number of SYN messages are sent to the victim and ends up using up all of the systems resources. **Countermeasures** • Decrease the connection-established timeout period (this will only lessen the effects of a SYN attack). • Increase the size of the connection queue in the IP stack. • Install proper patches. • Network IDS can watch for this activity and send alerts • FW can watch for these types of attacks and alert the admin or cut off the connection.
Teardrop	Sending very small packets that a system can not reassemble and causes a system to freeze or reboot. Systems usually only check to make sure that the packets are not too large, but do not check to see if they are too small. **Countermeasures** • Install patches or upgrade system • Disallow malformed fragments of packets to enter the environment • Use a router that will combine all fragments into full packets prior to routing to the

	destination system.
DDoS	**Distributed Denial of Service attack** – uses hundreds of thousands of computers to request services from a server or server farm until the system or web site is no longer functional. • Attacker creates master controllers that can in turn control slaves or zombie machines. • Master controller are systems that an attacker can achieve admin rights to so that programs can be loaded that will wait and listen for further instructions **Countermeasures:** • Perimeter routers restrict unnecessary ICMP and UDP traffic • A network IDS can be use to watch for this activity • Disable unused subsystems and services on computers • Rename admin account and implement strict password mgmt so systems cannot be used unknowingly • Packets that contain internal source IP addresses should not be accepted.
DNS DoS Attacks	Each DNS server is responsible for certain hosts, which are collectively referred to as a **Zone**. • If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert data into the cache of the server instead of replacing the actual records, which is referred to as **Cache poisoning.** • Many times the DNS server will cache previously resolved requests to make the next request for that hostname quicker. **Countermeasures:** • DNS should have public and internal records. The public records serve Internet requests and contain no sensitive info pertaining to the internal network. Internal records should be unreachable from the Inet • DNS servers should also be redundant by using a primary and secondary DNS server per zone • BIND versions should be updated • Employ secure DNS
Secure DNS	Primary DNS server make all the necessary changes to the records when host and/or IP addresses change and these records are then distributed to the secondary DNS servers. • If a secondary server received bogus records from an attacker instead of the primary DNS server, it would not know the difference and update its records • When Security DNS (DNSSEL) is implemented, the secondary DNS servers must authenticate the systems that are updating their records • Integrity checks are also performed to ensure that records were not modified or corrupted during transmission.
Timing Attacks	1. **B/t the lines entry attack** – The attacker taps into and uses an active communication line. User may not be using the connection at the time, but it is still acive, so the attacker jumps in and uses it. 2. **NAK/ACK attack** – A NAK is a negative acknowledgment to tell a system that a certain pice of info was not received or that a certain message parameter is unacceptable. Some systems do not deal with negative acknowledgements properly, and attackers use this weakness to their advantage. 3. **Line disconnect attack** – An attacker may access and keep a communication session open after the user attempts to terminate it.
Other	• DBMS is the SW that controls the access restrictions, data integrity, redundancy, and the different types of manipulation available for a DB • A relational DB uses 2 dimensional tables with rows (tuples) and columns (attributes). • A hierarchical DB uses a tree like structure to define relationships b/t data elements, uses a parent/child relationship • A distributed DB, or network DB has DB that are physically in different areas but logically connected to represent one main DB • DB integrity is provided by concurrency mechanisms. One concurrency control is locking, which prevents users from accessing and modifying data that is being used by someone else. • Entity integrity makes sure that a row, or tuple, is uniquely identified by a primary key, and referential integrity ensures that every foreign key refers to an existing primary key • 2 largest security problems associated w/ DB security are inference and aggregation • Risk mgmt and assessments should start at the beginning of a project and continue throughout the lifetime of the product • Change control needs to be put in place at the beginning of a project and must be enforced through each phase. • Changes must be authorized, tested, and recorded. Changes must not affect the security level of the system or its capability to enforce the security policy

	• Object oriented programming provides modularity, reusability and more granular control w/in the programs themselves • Objects are members, or instances, of classes. Classes dictate the objects' data type, structure, and acceptable actions. • A method is the functionality an object can carry out. • Objects can communicate properly b/c the are using standard interfaces. • Object oriented design represents a real world problem and modularizes the problem into cooperating objects that work together to solve the problem • An expert system uses a knowledge base full of facts, rules of thumb, and expert advice. It also has an inference machine that matches facts against patterns and determines which rules are to be applied. • A virus is an app that requires a host app for replication.

10. Operational Security

Topic	Description
Least Privilege	Least privilege and need-to-know are administrative controls • Means that an individual should have just enough permissions and rights to fulfill his role in the company and no more.
Security Operations and Product Evaluations	**Operational Assurance** – concentrates on the architecture of the product, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product. • Operational assurances examined in the eval process are access control mechanisms, separation of privileged and user program code, auditing and monitoring capabilities, cover channels, and trusted recovery **Life Cycle Assurance** – Pertains to how the product was developed and maintained. Each stage of the products life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product. • Examples are design specifications, clipping level config, unit and integration testing, configuration mgmt, and trusted distribution
Clipping Levels	The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. • Once the clipping level has been exceeded, further violations are recorded for review. • Most of the time IDS SW is used to track activities and behavior patterns • Clipping levels, auditing, and monitoring are done with the hope of discovering problems before major damage occurs.
Transparency	Security controls and mechanisms that are in place should have a degree of transparency that will allow a user to perform tasks and duties w/out having to go through extra steps b/c of security controls. • Transparency also does not let the user know too much about the controls, which helps prevent the user from figuring out how to circumvent them.
Change Mgmt Control	Change control is the mgmt of security features and a level of assurance provided through the control of the changes made to the system's HW, SW and firmware configurations throughout the development and operational life cycle. **Examples of the types of procedures that should be part of any change policy:** **1. Request for a change to take place** **2. Approval of the change** **3. Documentation of the change** **4. Tested and presented** **5. Implementation** **6. Report changes to mgmt**
Media Controls	**Sanitized** – When media is cleared of its contents. • Deleting files does not actually make the data disappear, it only deletes the pointers to where those files still live on the disk • **Data Remanence** – is the residual physical representation of info that was save and then erased in some fashion • A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero
System controls	To execute privileged HW instructions, a process must be running in a restrictive and protective state. This is an integral part of the OS architecture, and the determination of what processes can submit what type of instructions is made based on the OS control tables.

	• When a user program needs to send I/O info, it must notify the system's core, privileged processes that work at the inner rings of the system • These processes, called system services, either authorize the user program to perform these actions and temporarily increase their privileged state or the system's processes complete the request on behalf of the user program
Trusted Recovery	**3 types of trusted recovery:** 1. **System reboot** – takes place after shutting down the system in a controlled manner in response to a TCB failure • System goes into a maintenance mode and recovers from the actions taken. The system is brought up in a consistent and stable state. 2. **Emergency system restart** – takes place after a system failure happens in an uncontrolled manner • System goes into maintenance mode an recovers from the actions taken 3. **System cold start** – takes place when an unexpected TCB or media failure happens and the regular recovery procedure cannot recover the system to a more consistent state. • The system, TCB, and user objects may remain in an inconsistent state while the system attempts to recover itself • Intervention may be required by the user or Admin to restore the system
POP	**Post office Protocol** – an internet mail server protocol that supports incoming and outgoing messages. The mail server using POP stores and forwards e-mail messages and works w/ SMTP to move messages b/t mail servers
IMAP	**Internet Message Access Protocol** – an Internet protocol that enables users to access mail on a mail server • If a users are using POP when he accesses his mail server, all messages are automatically downloaded to his computer. Once they are downloaded from POP server they are usually deleted from the server • If a user uses IMAP they can download all messages or leave them on the mail server w/in there remote message folder, refered to as a mailbox
Email relaying	Mail servers use a **relay agent** to send a message from one mail server to another. This needs to be properly configured so that company's mail server is not used by another for spamming activity.
Facsimile Security	• Faxes just sitting in a bin that may contain sensitive info could be looked at by anyone • **Fax Servers** – some company's use, which is systems that manage incoming and outgoing faxed documents. When a fax is received by the fax server it properly routes it to the individual it is addressed to so that it is not actually printed, but held in electronic from • **Fax encryptor** – A bulk data link encryption mechanism. Encrypts any and all fax data that hits the network cable or telephone wire
Countermeasures to Port scanning and network mapping	• Disable unnecessary ports and services • Block access at the perimeter network using FW, routers, and proxy servers • Use an IDS to identify this type of activity • Use TCP Wrappers on vulnerable services that have to be available • Remove as many banners as possible w/in the OS and applications • Upgrade or update to more secure OS, apps and protocols **TCP Wrappers** – monitor incoming network traffic and control what can and cannot access the services mapped to specific ports. • When a request comes to a computer at a specific port, the target OS will check to see if this port is enable. • If it is enabled and the OS sees that the corresponding services is wrapped, it knows to look at an ACL, which spells out who can access this service.
Supperzapping	A utility used in IBM mainframes centers that has the capability to bypass access controls w/in the mainframes OS. • An admin would use this tool in the rare cases when nothing else seems to work and the system is malfunctioning, frozen, or entered a state that cannot be fixed by normal recovery procedures. • Today the superzapper term has been expanded upon to be any tool that can make modifications that are not auditable or logged.
Browsing	A general term used by intruders to obtain info that they are not authorized to access. This type of attack takes place when an attacker is looking for sensitive data, but does not know the format the data is in. • Another type of browing attack is **shoulder surfing**

Network sniffer	A tool that monitors traffic as it passes by. • Sniffers have been very successful b/c a majority of LANs use Ethernet, which is a broadcast technology. • Sniffers are becoming less successful b/c of the move to switched environments. • Switched environments break up broadcasts domains and collision domains. • **S-RPC** – Secure RPC – uses Diffie-Hellman public key cryptography to determin the share secret key for encryption with the DES algorithm • **r-utilities** – used in unix (rexex, rsh, rlogin, and rcp) are know to have several weaknesses. Should be replaced with SSH
Session Hijacking	If session hijacking is a concern the admin can implement a protocol that requires mutual authentication b/t users or systems like IPSec or Kerberos. B/c the attacker will not have the necessary credentials to authenticate to a user, the cannot act as an imposter and hijack sessions
Dictionary Attacks vs. Brute Force Attacks	**Dictionary Attack** – when a large lsit of words is fed into a password hacking tool and this tool runs a one-way hash on the captured password. Tool compares the hashing results to a password file to see if they match. **Brute-force attack** – A tool will try many different variations of characters, run a hash value on each variation and compare it to the hash value of the captured password. • A dictionary and brute force attack are usually used together. If a tool runs a dictionary attack and figures out the first few characters, the brute force will kick in and try different variations of the password until it finds a match.
Backdoors	Tools used for backdoor remote control actions are Back Orifice, Netbus, and sub seven
Attack types	**1. DoS** **2. Man-in-the middle** – Attacks can be countered with digital signatures and mutual authentication techniques **3. Spamming** – used to overwhelm a mail server. Email filtering and properly configuring mail relay functionality can protect against spamming **4. Wardialing** – Countermeasures are not to publicize these phone numbers and implement tight access control modems and modem pools **5. Ping of Death** – Oversized ICMP packets are sent to the victim. Systems that are vulnerable do not know how to handle oversized ICMP requests and may freeze or reboot. Countermeasures are patching and implementing ingress filtering to detect these types of attacks. **6. WinNuk** – DoS attack that sends out-of-band packets to port 139. Countermeasures are to patch or upgrade to a later OS **7. Fake login screens** – a HID can be used to detect this type of activity **8. Teardrop** – Countermeasures are patching the system and using ingress filtering to detect these packet types. **9. Traffic Analysis** – (sniffing) – traffic padding can be used to counter this which decoy traffic is sent out over the network to disguise patterns **10. Slamming and Cramming** – slamming is when a users telephone service provider has been changed w/out the users consent. Cramming is adding on charges that are bogus in nature that the user did not request.
Operations Security	Encompasses safeguards and countermeasures to protect resources, info, and the HW that they reside on. • Operations can pertain to SW, personnel, and HW • Mgmt is responsible for employees behavior and responsibilities • People w/in Ops are responsible for ensuring that systems are protected and that they continue to run a predictable manner
Unscheduled Initial Program Loads	**IPLs** – is a mainframe term for loading the OS's kernel into the computers main memory. • On a personnel computer, booting into the OS is the equivalent to IPLing. • This activity takes place to prepare the computer for user operation.
Other	• Sensitive info should contain the correct markings and labels to indicate the corresponding sensitivity levels • Contract and temp staff should have more restrictive controls put upon their accounts. • Media holding data must be properly purged, which could be zeroization, degaussing, or media destruction. • Ops dept is responsible for any unusual or unexplained occurrences, unscheduled initial program loads, and deviations from standards. • Supperzapper activities are not logged. • Improper mail relay configs allow for mail servers to be used to forward spam messages. • Main goal of operation security is to protect resources.
