CISSP

Domain 1

Security and Risk Management

(Security, Risk, Compliance, Law, Regulations, Business Continuity)

Key Areas for Domain 1

- CIA Triad
- Security Governance
- Compliance
- Legal and Regulatory Issues
- Professional Ethics
- Security Policy
- Business Continuity
- Personnel Security Policies
- Risk Management Concepts
- Threat Modeling
- Acquisition Strategy
- Training and Awareness

CIA Triad

- Confidentiality
- Integrity
- Availability

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Confidentiality

- Keep away from my stuff!!

- Privacy
  - Who has access to this material?
  - Supports Least Privilege

- Encryption is a good example of Confidentiality

Integrity

- The Trustworthiness of the data or a machine
- Did something change?
- How do we test for integrity?
    - Hashes?

Availability

- Hey data – are you there when I need you?

- Do you have your services up providing to your customers?
    - Heard of the five or six 9s?
        - 99.999% / 99.9999%

- What is one of the number one threats to our Availability?
    - Denial of Service attacks; Distributed DoS attacks

Security Governance

- Alignment of Security Functions
- Organizational Processes
- Security Roles and Responsibilities
- Control Frameworks
- Due Care
- Due Diligence

Alignment of Security Functions

- When it comes to IT, we used to be thought of as a back-office function
- We also just spent budget money and used company resources
  - Have to prove our worth
- Now days Cyber Security, Information Security, Security Governance are all the buzz words

Security Governance

- The intent of governance is to guarantee that the appropriate information security activities are being performed to ensure that the risks are appropriately reduced
- Information security investments are appropriately directed
  - Are we budgeting properly and spending wisely
- Executive management has visibility into the program and is asking the appropriate questions to determine the effectiveness of the program
  - Get them involved!

Alignment of Security Functions

- We want to line up our Information Security Management with the Mission, Goals and Objectives of the organization

- We can make assessments on risks and mitigation techniques then communicate them to upper management
  - The higher the better – want/need to be hear properly

Organizational Processes

- Businesses don’t always stay the same

- Things change from day to day and we have to be prepared

- Companies evolve and look to grow, change and become better
  - We have to be able to adapt and adjust to meet the organizational needs

Organizational Processes

- Acquisitions and Mergers – Organizations combine for many reasons. Some mergers are friendly with both parties realizing a gain from the merger, while others may be referred to as hostile
- What does this mean for us as a Security Manager?
  - More and/or new Vulnerabilities?
  - New threats?
  - New Policies?
  - Data type and/ or technology changes?
  - Business partner changes?

Organizational Processes

- Divestitures and Spinoffs – The opposite of an acquisition or a merger, a divesture may involve the spinoff of a part of an organization or possibly the complete liquidation of an existing organization
- Now we went the other way – what could that mean for us?
  - Data loss?
  - Threats by opened IT holes
  - Security holes by people/services missing

Organizational Processes

- Governance Committees – A governance committee is responsible for recruiting and maintaining the governance board for an organization.
- Responsible for determining missing qualifications and characteristics needed to enhance the efficiency and effectiveness of the board
  - Ensure the committee understands at a high level the importance of information security and risk management
  - Ensure committee recruitment exercises for new board members include requirements for information security and risk aptitude where needed.
  - Maintain a working relationship with committee members and be available to respond to specific risk, privacy, and information security questions as needed

Policies, Standards, Guidelines, and Procedures

- Policies, standards, guidelines, and procedures are all subtly different from each other, but they also interact with each other in a variety of ways.
- To successfully develop and implement information security policies, standards, guidelines, and procedures, you must ensure that your efforts are consistent with the organization's mission, goals, and objectives.

Policy Types

- Senior Management: A high-level management statement of an organization’s security objectives, organizational and individual responsibilities, ethics and beliefs, and general requirements and controls.
- Regulatory: Highly detailed and concise policies usually mandated by federal, state, industry, or other legal requirements.
- Advisory: Not mandatory, but highly recommended, often with specific penalties or consequences for failure to comply. Most policies fall into this category.
- Informative: Only informs, with no explicit requirements for compliance.

Security Roles and Responsibilities

- Security is the responsibility of everyone within the company!
- Every end-user is responsible for understanding the policies and procedures that are applicable to his or her particular job function and adhering to any and all security control expectations
- Users must have knowledge of their responsibilities and be trained to a level that is adequate to reduce the risk of loss to an acceptable level

Security Roles and Responsibilities

- Specific
  - Who is responsible for what for example, security updates, backups
- General
  - Who is responsible for security?
- Communicated at hiring
  - Need reminders & continuing education/awareness. Signing at hiring about liability.
- Verified capabilities and limitations
  - Don’t give people more access to anything than they need to do their jobs
- Third-party considerations
  - Vendors, Contractors, etc. Almost always have more rights & privileges. Should have least!
- Good practices
  - Security needs to be simple, relevant, understandable, and communicated. ISO is to make it easy and to make people understand why its important

Security Roles and Responsibilities - Internal

- Executive management
  - Has the ultimate responsibility for security breaches and results of the organization’s chosen risk mitigation strategies
- Information Systems Security Professionals/Information Security Officer
  - This one is us. Executive Management can only make good decisions if they get good advice. We are the ones they rely on for sound advice and guidance
    - Responsible for the design, implementation, management, review of the organization’s security policies, standards, baselines, procedures, and guidelines
- Developers
  - Systems designers & developers, particularly software developers
- Custodians & Operations staff
  - Largely the people who maintain our systems

Security Roles and Responsibilities - Internal

- Security staff / Physical Security
- Data and system owners
  - Information classification, defining and deciding user access
- End Users
- Legal, compliance, and privacy officer
  - Laws and regulations etc. & make sure that the policies & procedures in place support.
- Internal auditors

Security Roles and Responsibilities - External

- Vendors/suppliers
- Contractors
- Temporary employees
- Customers
- Business partners
- Outsourced relationships

Control Frameworks

- To make sure we as Information Security Officers are doing what we are supposed to be doing for security
  - Have a framework in place to maintain the governance
  - Consistent – A governance program must be consistent in how information security and privacy is approached and applied
  - Measurable – The governance program must provide a way to determine progress and set goals
  - Standardized – Results from one organization or part of an organization can be compared in a meaningful way
  - Comprehensive – The selected framework should cover the minimum legal and regulatory requirements of an organization and be extensible to accommodate additional organization-specific requirements
  - Modular– A modular framework is more likely to withstand the changes of an organization since only the controls or requirements needing modification are reviewed and updated

Due Diligence

- Is the enforcement of due care policy and provisions to ensure that the due care steps taken to protect assets are working effectively
- Identifying what we need for Security
- Are we protecting our organization?
  - Penetration testing
  - Vulnerability scans
  - Internal Audits

Due Care

- Organization's Management "exercise the care which ordinarily prudent and reasonable persons would exercise under the same circumstances"
- Are you doing what you are supposed to be doing to protect our company?
- Might be under legal obligation to "Do the right thing!"

Coming Up!

- Next we will continue with Domain 1 starting with Compliance.

*

Compliance

- Legislative and Regulatory Compliance
- Privacy Requirements

Legislative and Regulatory Compliance

- Many laws out there have to be followed and ISO need to be familiar with them.
- Some companies hire dedicated employees to keep up with regulations
  - Want companies to follow the law

- Payment Card Industry Data Security Standard (PCI DSS)
  - Applies to any business worldwide that transmits, processes, or stores payment card (meaning credit card) transactions to conduct business with customers’ whether that business handles thousands of credit card transactions a day or a single transaction a year.

Privacy Requirements

- Organizations collect tons of data and that data is shared or can be; Some data needs to stay private!
- Several pieces of privacy and data protection legislation include the:
    - Federal Privacy Act
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Health Information Technology for Economic and Clinical Health Act (HITECH)
    - Gramm-Leach-Bliley Act (GLBA) in the United States
    - Data Protection Act (DPA) in the United Kingdom

Legal and Regulatory Issues

- Computer Crimes
- Licensing and Intellectual Property
- Import/Export Controls
- Trans-border Data Flow
- Privacy
- Data Breaches

Computer Crimes

- Computer crime consists of any criminal activity in which computer systems or networks are used as tools
- Simply put, a computer crime is a crime (or violation of a law or regulation) that involves a computer.
- There are many ways to attack a computer system and many motivations to do so
- Information system security practitioners generally put crimes against or involving computers into different categories
- The crime could be against the computer, or the computer could have been used in the actual commission of the crime

Computer Crimes

- Some Types
  - Business
  - For fun
  - Upset or disgruntled employees
  - Cyber Terrorism
  - Financial Attacks
  - Personal Attacks

Licensing and Intellectual Property

- Intellectual Property
  - How you are perceived due to your past accomplishments
  - Property you have created and is “yours”
  - Could be part of your brand
- Intellectual property laws are designed to protect both tangible and intangible items and property

Patents

- Patents protect novel, useful, and non-obvious inventions
- Patents are the strongest form of intellectual property protection
- The patent owner has a legally enforceable right to prevent others from using the patented invention for a specific period of time (usually 20 years)
- Once a patent is granted, it is published in the public domain in order to stimulate other innovations

Trademark

- Projects the “good will” that merchants or vendors invest in the recognition of their products
- Gives the owner of the markings exclusive rights over the item for which the trademark was granted
- Trademarks are registered with a government registrar

Copyright

- Copyright covers the expression of ideas
- Rather than the ideas themselves, it protects artistic property such as writings and recordings, and protects computer programs from direct copying of the source code or software logic
- **Work for Hire:** Work done by an employee of a company as part of the employee's duties or using specialized equipment owned by the company created intellectual property that belongs to the employer.

Trade Secrets

- Intellectual property refers to proprietary business or technical information, processes, designs, practices, etc., that are confidential and critical to the business

- Think about Coca-Cola and KFC

Licensing

- Are you and/or you organization within legal requirements of licensing for software?

- Freeware
- Shareware
- Commercial
- Academic

Import/Export Controls

- The government understands computers are powerful and early on adopted some laws to prevent the exporting of system to other countries that could pose threats to the US
  - International Traffic In Arms Regulations (ITAR)
    - What is a defense item and what can be done (Presidential Decision)
  - Export Administration Regulations (EAR)
    - Regulate exports of civilian goods and technologies (equipment, materials, software, and technology, including data and know-how) that have military applications (Presidential Decision)

Trans-border Data Flow

- Moving data between country borders from server to server
  - Who has regulation jurisdiction?
  - Which laws do we have to follow?
    - Countries laws where the data is stored or the country the owning company resides with?

- Tons of information is being collected from web, RFID chips, and search engines

- Can be used to fight Cyber Terrorism

Privacy

- PII – Personal Identifiable Information
    - Information about YOU!
    - Protect this information
        - SSN, Phone Number, Bank Account Numbers, etc…
- Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information
- Personal information is a rather generic concept and encompasses any information that is about or on an identifiable individual
- The Organization for Economic Cooperation and Development (OECD) has broadly classified these principles into the collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability

Data Breaches

- An incident that results in the disclosure or potential exposure of data

- Hear about these almost quarterly if not monthly anymore
  - Target, Home Depot, eBay, Veterans Affairs, on and on

Coming Up!

- Next we are going to continue on with Domain 1 starting off with Understanding Professional Ethics

*

Professional Ethics

- Code of Professional Ethics
- Supporting Organizations’ Code of Ethics

Code of Professional Ethics

- Preamble:
    - The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
    - Therefore, strict adherence to this Code is a condition of certification.
- Canons:
    - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
    - Act honorably, honestly, justly, responsibly, and legally.
    - Provide diligent and competent service to principals.
    - Advance and protect the profession.

Supporting Organizations’ Code of Ethics

- Develop a corporate guide to computer ethics for the organization
- Develop a computer ethics policy to supplement the computer security policy
- Add information about computer ethics to the employee handbook
- Find out whether the organization has a business ethics policy, and expand it to include computer ethics
- Learn more about computer ethics and spreading what is learned
- Help to foster awareness of computer ethics by participating in the computer ethics campaign
- Make sure the organization has an E-mail privacy policy
- Make sure employees know what the E-mail policy is

Security Policy

- Policies
- Standards
- Procedures
- Guidelines

Policies

- A security policy is a document that defines the scope of security needed by the organization and discusses the assets that need protection and the extent to which security solutions should go to provide the necessary protection
- The security policy is an overview or generalization of an organization's security needs
- Defines the main security objectives and outlines the security framework of an organization
- Identifies the major functional areas of data processing and clarifies and defines all relevant terminology
- Should clearly define why security is important and what assets are valuable

Policies, Standards, Guidelines, and Procedures

- Standards (and baselines)
  - Standards are specific, mandatory requirements that further define and support higher-level policies. For example, a standard may require the use of a specific technology, such as a minimum requirement for encryption of sensitive data using 3DES. A standard may go so far as to specify the exact brand, product, or protocol to be implemented.
  - Baselines are similar to and related to standards. A baseline can be useful for identifying a consistent basis for an organization's security architecture, taking into account system-specific parameters, such as different operating systems. After consistent baselines are established, appropriate standards can be defined across the organization.

Policies, Standards, Guidelines, and Procedures

- Guidelines
  - Guidelines are similar to standards but they function as recommendations rather than as compulsory requirements. For example, a guideline may provide tips or recommendations for determining the sensitivity of a file and whether encryption is required.
- Procedures
  - Procedures provide detailed instructions on how to implement specific policies and meet the criteria defined in standards. Procedures may include Standard Operating Procedures (SOPs), run books, and user guides. For example, a procedure may be a step-by-step guide for encrypting sensitive files by using a specific software encryption product.

Business Continuity

- Project Scope and Plan
- Business Impact Analysis

BCP – Business Continuity Plan

1. Analyze your business
2. Assess the risks
3. Develop your strategy
4. Develop your plan
5. Rehearse the plan

Analyze the Business

- This is the first stage of the business continuity management life cycle, as it is necessary to understand at the outset exactly where your business is vulnerable
- You will need the fullest possible understanding of the important processes inside your organization and between you and your customers and suppliers

Assess the risks

- There are two aspects to every risk to your organization:
  - How likely is the risk to happen?
  - What effect will it have on your organization?

Develop your strategy

- Whatever type of organization you are, you will probably choose one of the following strategies:
  - Accept the risks – change nothing
  - Accept the risks with an arrangement for help after an incident
  - Attempt to reduce the risks
  - Attempt to reduce the risks and make arrangements for help after an incident
  - Reduce all risks to the point where you should not need outside help

Develop your plan

- Once your strategy has been decided upon, the plan can be put in place
- Business continuity management plans will look different for different organizations
  - BCP should provide:
    - For an immediate, accurate, and measured response to emergency situations
    - Policies, procedures, and documentation needed to assist in the recovery process
    - A database of resources available to aid the recovery process
    - An approved list of vendors that may be able to help during the recovery process
    - Needed documents and agreements required to reduce outages; aka “SLAs” (service level agreements)

Rehearse the plan

- Practice makes perfect!
- The BC plan is a living document, and sometimes you only discover any weaknesses in it when you put it into action
- Rehearsal helps you confirm that your plan will be connected and robust if you ever need it; rehearsals are also good ways to train staff to have business continuity responsibility

Business Impact Analysis - BIA

- Identify discrete business activities and the owners of these processes
- Identify suitable staff from whom the information can be sought about the business processes
- Identify impacts that might result in damage to the organization's reputation, assets, or financial position
- Quantify the timescale within which the interruption of each business activity becomes unacceptable to the organization
- Workshops, questionnaires, interviews, observation

Business Impact Analysis - BIA

- A BIA predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies
- Potential loss scenarios should be identified during a risk assessment
- Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries

Personnel Security Policies

- Candidate Screening
- Employment Agreements and Policies
- Termination Processes
- Vendor, Consultant, and Contractor Controls
- Compliance
- Privacy

Candidate Screening

- Reference checks
- Education verification
- Background Investigations
  - Job duties
  - Salary
  - Reasons for leaving a job
  - Validity and status of professional certification
  - Education verification and degrees obtained
  - Credit history
  - Driving records
  - Criminal history
  - Personal references
  - Social security number verification

Employment Agreements and Policies

- Employment agreements are usually signed by the employee before he or she starts the new job or during his or her first day
- Usually their purpose is to protect the organization while the individual is employed, as well as after the employee has left employment by the organization

Employment Agreements and Policies

- Job Rotation
- Separation of Duties
- Least Privilege
- Mandatory Vacations

Termination Processes

- Friendly vs Unfriendly

- Friendly Termination
  - Exit interview
  - NDA Reminder
  - Collect access badges, tokens, cards, etc…
- Unfriendly Termination
  - Disable accounts immediately
  - Escort from building

Vendor, Consultant, and Contractor Controls

- When it comes to Vendors, Consultants and/or Contractors the same controls (if not more) need to be in place as for regular employees

- These individuals have access to data, data systems and other personnel

- Escorts
- Monitoring
- NDA

Privacy

- Privacy is something everyone expects but when is it “okay” for employers to monitor employees and how far?
- CCTV okay in office area? Break area?
- Monitoring teleworkers in their home office?

Coming Up!

- Next we will continue with Domain 1 talking about the big topic of Risk Management

Risk Management Concepts

- Threats and Vulnerabilities
- Risk Assessment/Analysis
- Risk Assignment/Acceptance
- Countermeasures
- Implementation
- Types of Controls
- Control Assessment
- Monitoring and Measurement
- Asset Valuation
- Reporting
- Continuous Improvement
- Risk Frameworks

Risk Management Concepts

- **Risk**—A risk is a function of the likelihood of a given threat source's exercising a potential vulnerability, and the resulting impact of that adverse event on the organization.
- **Likelihood**—The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.
- **Threat Source**—Either intent and method targeted at the intentional exploitation of a vulnerability or a situation or method that may accidentally trigger a vulnerability.
- **Threat**—The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Risk Management Concepts

- **Vulnerability**—A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.
- **Impact**—The magnitude of harm that could be caused by a threat’s exercise of a vulnerability.
- **Asset**—Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

Risk Management Concepts

- **Safeguards -** A safeguard, or countermeasure, is anything that removes or reduces a vulnerability or protects against one or more specific threats.
- Can be installing a software patch, making a configuration change, hiring security guards, altering the infrastructure, modifying processes, improving the security policy, training personnel more effectively, electrifying a perimeter fence, installing lights, and so on
- Any action or product that reduces risk through the elimination or lessening of a threat or a vulnerability anywhere within an organization.
- Important to remember that a safeguard, security control, or countermeasure need not involve the purchase of a new product; reconfiguring existing elements or even removing elements from the infrastructure are also valid safeguards.

Risk Management Concepts

- **Attack** - An attack is the exploitation of a vulnerability by a threat agent. In other words, an attack is any intentional attempt to exploit a vulnerability of an organization's security infrastructure to cause damage, loss, or disclosure of assets. An attack can also be viewed as any violation or failure to adhere to an organization's security policy.
- **Breach** - A breach is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. When a breach is combined with an attack, a penetration, or intrusion, can result. A penetration is the condition in which a threat agent has gained access to an organization's infrastructure through the circumvention of security controls and is able to directly imperil assets.

Risk Management Concepts

- **Mean Time Between Failures (MTBF)**
  - The measure of the anticipated incidence of failure for a system or component, defines reliability
- **Mean Time to Failure (MTTF)**
  - The average time to failure for a non-repairable system
- **Mean Time To Restore (MTTR)**
  - The measurement of how long it takes to repair a system or component once a failure occurs

Risk Management Concepts

- **Recovery Time Objectives (RTO)**
  - The maximum down time considered acceptable for a process or service
- **Recovery Point Objective (RPO)**
  - Defines the point to which a crashed or failed system needs to be restored

Threat Sources

- **Human** – Malicious outsider, malicious insider, (bio) terrorist, saboteur, spy, political or competitive operative, loss of key personnel, errors made by human intervention, cultural issues
- **Natural** – Fire, flood, tornado, hurricane, snow storm, earthquake.
- **Technical** – Hardware failure, software failure, malicious code, unauthorized use, use of emerging services, such as wireless, new technologies.
- **Physical** – Closed-circuit TV failure due to faulty components, perimeter defense failure.
- **Environmental** – Hazardous waste, biological agent, utility failure.
- **Operational** – A process (manual or automated) that affects confidentiality, integrity, or availability.

Risk Management Process

- Risk management is the process of
  - Identifying risks
  - Assessing their potential impacts to the organization
  - Determining the likelihood of their occurrence
  - Communicating findings to management and other affected parties
  - Developing and implementing risk mitigation strategies to reduce risks to levels that are acceptable to the organization

Risk Assessment/Analysis

- The quantitative method results in concrete probability percentages. That means the end result is a report that has dollar figures for levels of risk, potential loss, cost of countermeasures, and value of safeguards.
- This report is usually fairly easy to understand, especially for anyone with knowledge of spreadsheets and budget reports.
- Quantitative analysis as the act of assigning a quantity to risk; in other words, placing a dollar figure on each asset and threat
  - However, a purely quantitative analysis is not sufficient; not all elements and aspects of the analysis can be quantified because some are qualitative, subjective, or intangible

Quantitative Analysis

- The exposure factor (EF) represents the percentage of loss that an organization would experience if a specific asset were violated by a realized risk. The EF can also be called the loss potential. In most cases, a realized risk does not result in the total loss of an asset. The EF simply indicates the expected overall asset value loss because of a single realized risk. The EF is usually small for assets that are easily replaceable, such as hardware. It can be very large for assets that are irreplaceable or proprietary, such as product designs or a database of customers. The EF is expressed as a percentage.
- Single loss expectancy
    - The EF is needed to calculate the SLE. The single loss expectancy (SLE) is the cost associated with a single realized risk against a specific asset. It indicates the exact amount of loss an organization would experience if an asset were harmed by a specific threat occurring.
- The SLE is calculated using the following formula:
    - SLE = asset value (AV) * exposure factor (EF)
    - SLE = AV * EF

Quantitative Analysis

- The annualized rate of occurrence (ARO) is the expected frequency with which a specific threat or risk will occur (that is, become realized) within a single year. The ARO can range from a value of 0.0 (zero), indicating that the threat or risk will never be realized, to a very large number, indicating that the threat or risk occurs often.
- Calculating the ARO can be complicated. It can be derived from historical records, statistical analysis, or guesswork. ARO calculation is also known as probability determination.
- The annualized loss expectancy (ALE) is the possible yearly cost of all instances of a specific realized threat against a specific asset.
- The ALE is calculated using the following formula:
  - ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO)
  - ALE = SLE * ARO

Qualitative & Hybrid Analysis

- Qualitative risk analysis is more scenario based than it is calculator based. Rather than assigning exact dollar figures to possible losses, you rank threats on a scale to evaluate their risks, costs, and effects.
- Since a purely quantitative risk assessment is not possible, balancing the results of a quantitative analysis is essential.
- The method of combining quantitative and qualitative analysis into a final assessment of organizational risk is known as **hybrid** assessment or hybrid analysis.
- The process of performing qualitative risk analysis involves judgment, intuition, and experience

Risk Assignment/Acceptance

- **Risk Avoidance**
  - Involves identifying a risk and making the decision to no longer engage in actions associated with that risk.
- **Risk Transference**
  - Sharing some of the burden of the risk with someone else.
- **Risk Mitigation**
  - Accomplished anytime steps are taken to reduce risk

Risk Assignment/Acceptance

- **Risk Deterrence**
  - Involves understanding something about the enemy and letting them know harm can come their way if they cause harm to you.
- **Risk Acceptance**
  - Often the choice that must be made when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition.

Risk Assignment/Acceptance

- Who is assigned the risk?

- Company?
- Individuals?

Countermeasures

- Accountability (can be held responsible)
- Auditability (can it be tested?)
- Trusted source (source is known)
- Independence (self-determining)
- Consistently applied
- Cost-effective
- Reliable
- Independence from other countermeasures (no overlap)
- Ease of use
- Automation
- Sustainable
- Secure
- Protects confidentiality, integrity, and availability of assets
- Can be “backed out” in event of issue
- Creates no additional issues during operation
- Leaves no residual data from its function

Implementation

- Who ?
- What ?
- Why ?
- When ?
- Where ?
- How ?
- Budget ?

Types of Controls

- **Preventive access control** - deployed to thwart or stop unwanted or unauthorized activity from occurring. Examples of preventive access controls include fences, locks, biometrics, mantraps, lighting, alarm systems, separation of duties, job rotation, data classification, penetration testing, access control methods, encryption, auditing, presence of security cameras or closed circuit television (CCTV), smart cards, callback procedures, security policies, security awareness training, antivirus software, firewalls, and intrusion prevention systems.

Types of Controls

- **Detective access control** - deployed to discover or detect unwanted or unauthorized activity. Detective controls operate after the fact and can discover the activity only after it has occurred. Examples of detective access controls include security guards, motion detectors, recording and reviewing of events captured by security cameras or CCTV, job rotation, mandatory vacations, audit trails, honeypots or honeynets, intrusion detection systems, violation reports, supervision and reviews of users, and incident investigations.
- **Corrective access control** - modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred. They attempt to correct any problems that occurred as a result of a security incident. Corrective controls can be simple, such as terminating malicious activity or rebooting a system. They also include antivirus solutions that can remove or quarantine a virus, backup and restore plans to ensure that lost data can be restored, and active intrusion detection systems that can modify the environment to stop an attack in progress.

Types of Controls

- **Deterrent access control** - deployed to discourage violation of security policies. Deterrent and preventive controls are similar, but deterrent controls often depend on individuals deciding not to take an unwanted action. In contrast, a preventive control actually blocks the action. Some examples include policies, security awareness training, locks, fences, security badges, guards, mantraps, and security cameras.
- **Directive access control** - deployed to direct, confine, or control the actions of subjects to force or encourage compliance with security policies. Examples of directive access controls include security policy requirements or criteria, posted notifications, escape route exit signs, monitoring, supervision, and procedures.

Types of Controls

- **Recovery access control** - deployed to repair or restore resources, functions, and capabilities after a violation of security policies. Recovery controls are an extension of corrective controls but have more advanced or complex abilities. Examples of recovery access controls include backups and restores, fault-tolerant drive systems, system imaging, server clustering, antivirus software, and database or virtual machine shadowing.
- **Compensation access control** - deployed to provide various options to other existing controls to aid in enforcement and support of security policies. They can be any controls used in addition to, or in place of, another control. For example, an organizational policy may dictate that all personally identifiable information (PII) must be encrypted. A review discovers that a preventive control is encrypting all PII data within databases, but PII transferred over the network is sent in cleartext. A compensation control would be added to protect the data in transit.

How are Controls Applied

- **Administrative controls** - the policies and procedures defined by an organization's security policy and other regulations or requirements. They are sometimes referred to as management controls. These controls focus on personnel and business practices. Examples of administrative access controls include policies, procedures, hiring practices, background checks, data classifications and labeling, security awareness and training efforts, vacation history, reports and reviews, work supervision, personnel controls, and testing.
- **Logical/technical controls (also known as technical access controls)** - the hardware or software mechanisms used to manage access and to provide protection for resources and systems. As the name implies, they use technology. Examples of logical or technical access controls include authentication methods (such as usernames, passwords, smart cards, and biometrics), encryption, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

How are Controls Applied

- **Physical controls** - items you can physically touch. They include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, video cameras, mantraps, and alarms.

Control Assessment

- Verifying that the implementers and operators of information systems are meeting their stated security goals and objectives

- Findings are used to determine the overall effectiveness of the security controls associated with an information system (including system-specific, common, and hybrid controls) and to provide credible and meaningful inputs to the organization's risk management process

Monitoring and Measurement

- How can we Measure if the controls are working?

- Vulnerability scans
- Penetration testing

Asset Valuation

- Tangible assets
  - Something you can touch
    - hardware, software, facilities, customer lists, intellectual property

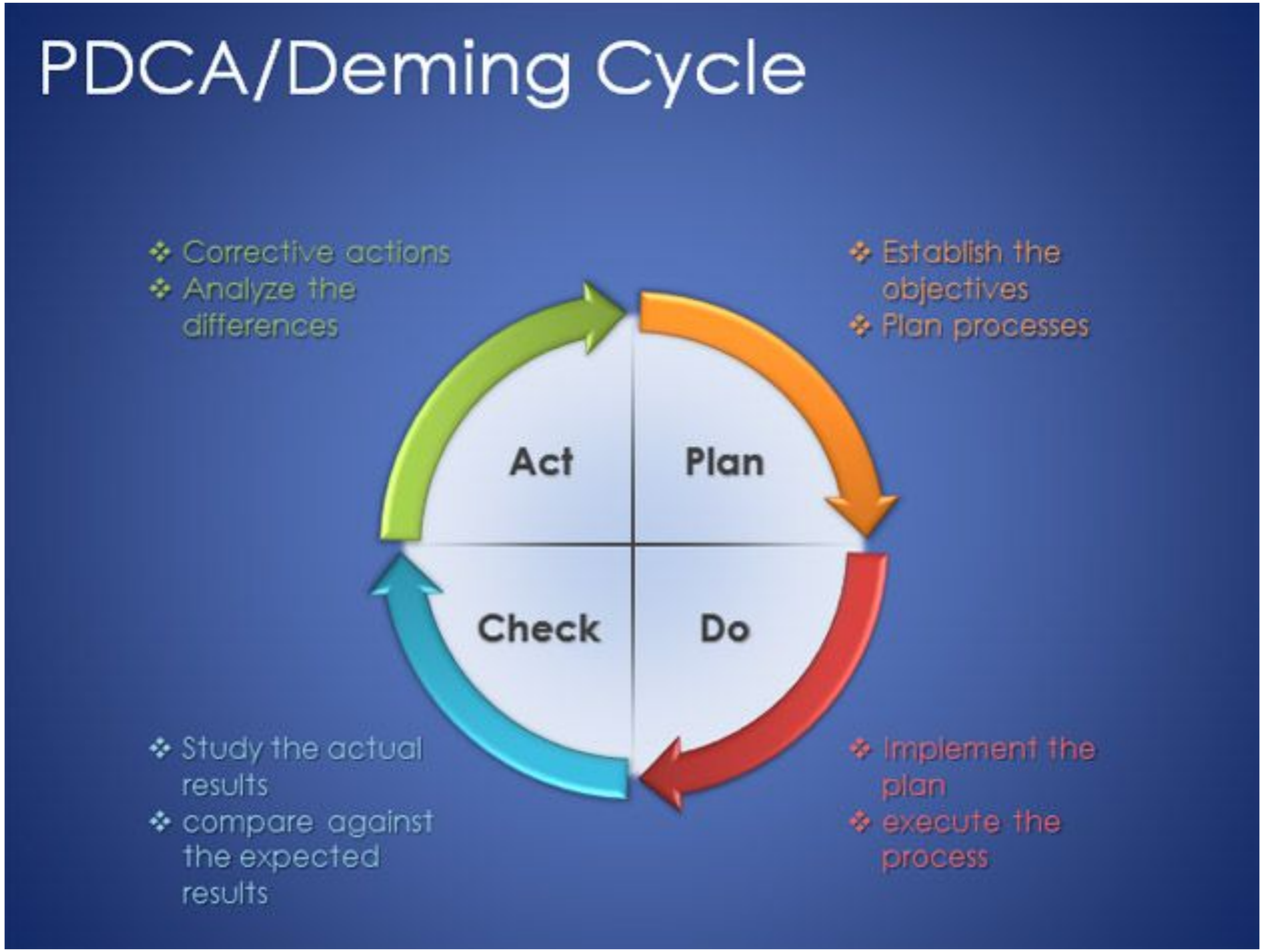
- Intangible assets
  - Unable to be touched or grasped
    - Employee MORALE, reputation/brand, Customer satisfaction

Reporting

- Reporting our Risk Analysis needs to go as high up the chain as possible

- Depending on the report audience the ISO needs to understand terminology and how to explain technical topics in every day terms

Continuous Improvement



PDCA/Deming Cycle

- Establish the objectives
- Plan processes

- Implement the plan
- execute the process

- Study the actual results
- compare against the expected results

- Corrective actions
- Analyze the differences

Risk Frameworks

- The policy, objectives, mandate, and commitment to manage risk.

- The organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities and should be embedded within the organization's overall strategic and operational policies and practices

Security Program Framework

- An organization’s security program should be tailored to the specific needs of the business, taking into consideration its overall mission, business objectives, operating climate, and strategic and tactical plans
- Many frameworks for use to follow
  - ISO/IEC 27002 Code of Practice for Information Security Management—
    - This international standard, jointly issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provides a best practices framework for implementing and managing an information security program

Security Program Framework

- The ISO/IEC 27001 provides more detailed implementation guidance for the security practitioner, and defines the requirements for a formal specification of an Information Security Management System (ISMS) that can be independently certified.
- More of a standard compared to the 27002 guideline
- Plan, Do, Check, Act

Coming Up!!

- Coming up next we will wrap up Domain 1 starting with Threat Modeling

*

Threat Modeling

- Identifying Threats
- Potential Attacks
- Reduction Analysis
- Remediating Threats

Identifying Threats

- Threat modeling is a procedure for optimizing Network/ Application/ Internet Security by identifying objectives and vulnerabilities and then defining countermeasures to prevent, or mitigate the effects of, threats to the system
- A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental

Threat Modeling Process

- **Assessment Scope** – Identifying tangible assets like databases of information or sensitive files is usually easy. Understanding the capabilities provided by the application and valuing them is more difficult. Less concrete things such as reputation and goodwill are the most difficult to measure, but they are often the most critical
- **Possible Attacks** – A key part of the threat model is a characterization of the different groups of people who might be able to attack an application. These groups should include insiders and outsiders, performing both inadvertent mistakes and malicious attacks
- **Countermeasures** – The model must include any and all existing countermeasures already deployed within the enterprise.

Threat Modeling Process

- **Vulnerabilities** – Once you have an understanding of the security in the application, you can then analyze for new vulnerabilities. The focus needs to be on vulnerabilities that connect the possible attacks that you have identified to the negative consequences that you have identified.
- **Prioritized Identified Risks** – Prioritization is everything in threat modeling because there are always lots of risks that simply do not rate any attention. For each threat, you estimate a number of likelihood and impact factors to determine an overall risk or severity level.
- **Identify Countermeasures to Reduce Threat** – The last step is to identify countermeasures to reduce the risk to acceptable levels, based on the risk appetite of the enterprise.

Potential Attacks

- Tailgating
- Phishing
- Social Engineering
- Baiting

Reduction Analysis

- How Does an Individual Avoid Being a Victim?

- How Can Organizations Reduce Their Security Risks?

Remediating Threats

- Go Away Threats!

- Policies
- IDS/IPS
- Firewalls
- Encryption
- Security Protocols (SSL/TLS/IPSec)
  - Tunneling

Acquisition Strategy

- Hardware, Software and Services
- Third-party Assessment and Monitoring
- Minimum Security Requirements
- Service-level Requirements

Hardware, Software and Services

- For hardware, software and services we need to have redundancy and diversity for the organization
- It’s hard to stop all attacks and we don’t want all our eggs in one basket (vendor)
- Hardware vendors need to meet security requirements for the organization
- Service providers, cloud providers, etc… need to meet the organization’s security requirements as well
- Only as strong as our weakest link

Third-party Assessment and Monitoring

- Third-party governance is the system of oversight that may be mandated by law, regulation, industry standards, or licensing requirements.
- The actual method of governance may vary but it generally involves an outside investigator or auditor.
    - These auditors might be designated by a governing body or might be consultants hired by the target organization.
- Another aspect of third-party governance is the application of security oversight on third parties that your organization relies upon
- Many organizations choose to outsource various aspects of their business operations
    - Outsourced operations can include security guards, maintenance, technical support, and accounting services.
- These parties need to stay in compliance with the primary organization’s security stance. Otherwise, they present additional risks and vulnerabilities to the primary organization.

Third-party Assessment and Monitoring

- Documentation review is the process of reading the exchanged materials and verifying them against standards and expectations
- The documentation review is typically performed before any on-site inspection takes place
- If the exchanged documentation is sufficient and meets expectations (or at least requirements), then an on-site review will be able to focus on compliance with the stated documentation

Minimum Security Requirements

- What are they?

- Make a list of the requirements then tie the security requirements to them

Service-level Requirements

- The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers
- Contains the requirements of the IT service from the client viewpoint
- Becomes draft of our Service Level Agreement

Training and Awareness

- Appropriate Levels
- Periodic Reviews

User Education and Awareness

- Before we dive into Training we have to think of our audience
  - Who are we training?
    - Business Users?
    - Technical Staff?
    - Management?
  - Each audience group has different outlooks, different skill sets and will need to be educated somewhat differently

- Good starting point of training for an organization is training on Policies – Security Policies

User Education and Awareness

- How are we going to deliver training?
  - Seminars
  - Lunch and Learn
  - Computer Based Learning
  - Intranet Sites
  - Videos on Demand (Previously recorded sessions)

User Education and Awareness

- What are going to try and cover first?
  - User Habits!
    - Password Behavior
      - Strong passwords; Keep it secret
    - Data Handling or Lack Of
      - Encryption; Data destruction; What type of devices to use or not use
    - Clean Desk Policy
      - Don’t leave sensitive data laying around
    - Tailgating
      - Someone just walking in behind you to bypass physical security
    - Personally Owned Devices / BYOD
      - Does your organization allow them

User Education and Awareness

- New Threats and Security Trends
  - Be sure to talk about the latest and "greatest" out there
    - Latest phishing attacks? Zero days?
  - What are the trends for attackers now days?
    - Social engineering? Malware?
- Use of Social Networking and P2P
  - Make sure we train on awareness and dangers of social media
    - FB, Twitter, Instagram, etc…
    - Don't share too much information
  - P2P sites can transmit viruses and malware like wild fire
    - What you are downloading could be against the law as well!

User Education and Awareness – Other Topics

- Social engineering
- Business continuity
- Disaster recovery
- Emergency management, to include hazardous materials, biohazards, etc
- Security incident response
- Risk assessment

- Data classification
- Information labeling and handling
- Personnel security, safety, and soundness
- Physical security
- Appropriate computing resource use
- Accidents, errors, or omissions

Periodic Reviews

- We are done with training, now what?

- Get some training metrics
  - See how well you did on your training
  - How well did they listen or understand what you were putting out

- Follow up
  - See if the attendees have any further questions

Domain 1 Complete!

- CIA
- Security Governance
- Compliance
- Legal and Regulatory Issues
- Professional Ethics
- Security Policy
- Business Continuity
- Personnel Security Policies
- Risk Management Concepts
- Threat Modeling
- Acquisition Strategy
- Training and Awareness

CISSP

Asset Security

(Protecting Security of Assets)

Key Areas

- Classify information and supporting assets
- Determine and maintain ownership
- Protect Privacy
- Ensure appropriate retention
- Determine data security controls
- Establish handling requirements

Classify information and supporting assets

- Classification is most often referred to when discussing military or government information; however several organizations may use systems that are similar in function
- Classification system is to ensure information is marked in such a way that only those with an appropriate level of clearance can have access to the information.

Data Classifications

- **Top Secret**—Disclosure could result in exceptionally grave damage to national or international security. Examples include vital military intelligence data, cryptographic keys used to protect communications, and detailed weapons design.
- **Secret**—Disclosure could seriously damage national security. Examples include significant intelligence and military plans and information, technical developments, and diplomatic strategies.
- **Confidential**—Disclosure could cause damage to national security. Examples include tests of military strength, performance data, and technical training and operations documents.

Data Classifications

- **Sensitive but Unclassified**—Information that is not classified top secret, secret, or confidential but whose dissemination is still restricted to protect national interests.
- **Unclassified**—In general, this information is publicly available through the Freedom of Information Act, although special classifications such as “Unclassified—For Law Enforcement Only” may be assigned to restrict disclosure to certain organizations with a need to know.

Determine and maintain ownership

- Data Owners:
  - When information is created, someone in the organization must be directly responsible for it
  - This is often the individual or group that created, purchased, or acquired the information to support the mission of the organization.
  - This individual or group is considered the “information owner.”

- Data custodians are established to ensure that important datasets are developed, maintained, and are accessible within their defined specifications

Protect Privacy

- Data Owners
- Data Processors
- Data Remanence
- Collection Limitation

Data Owners

- A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

- Data protection laws tend to converge around the principle that individuals should have control over their personal information

Data Processors

- In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data Remanence

- Data remanence is the residual physical representation of data that has been in some way erased
- Once storage media is erased, there may be some physical characteristics that allow data to be reconstructed

Collection Limitation

- Obtained fairly and lawfully
- Used only for the original specified purpose
- Adequate, relevant, and not excessive to purpose
- Accurate and up to date
- Accessible to the subject
- Kept secure
- Destroyed after its purpose is completed

Ensure appropriate retention

- Information and data should be kept only as long as it is required.
- Organizations may have to keep certain records for a period as specified by industry standards or in accordance with laws and regulations
- Hard- and soft-copy records should not be kept beyond their required or useful life

Ensure appropriate retention

- Record retention policies indicate how long an organization must maintain copies of information
- For example, financial transactions related to a fraud case may need to be retained indefinitely or until ten years after a court judgment
- Other information such as system logs may need to be retained for six months or longer to ensure appropriate forensics and incident response capabilities can use the information to reconstruct a past event

Determine data security controls

- Baselines
- Scoping and Tailoring
- Standards Selection
- Cryptography

Baselines

- Effective network security demands an integrated defense-in-depth approach
- The first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security
- These fundamental security elements form a security baseline, creating a strong foundation on which more advanced methods and techniques can subsequently be built
- The objective of baseline protection is to establish a minimum set of safeguards to protect all or some of the IT systems of the enterprise

Baselines

- An enterprise may also generate its own baseline

- One such example of this approach can be found by examining the United States Government Configuration Baseline (USGCB)
- The purpose of the USGCB initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies

Scoping and Tailoring

- Scoping guidance provides an enterprise with specific terms and conditions on the applicability and implementation of individual security controls
- System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made

Scoping and Tailoring

- Tailoring involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation
- The tailoring process gives enterprises the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts of a risk management framework

Standards Selection

- The security practitioner needs to be familiar with a wide range of standards and the organizations and entities that are responsible for them
    - US based entities such as NIST
    - Transnational entities:
        - European Network and Information Security Agency (ENISA)
        - The International Telecommunications Union (ITU)
        - The International Standards Organization (ISO)

Cryptography

- Cryptography is the art of hiding information in plain sight
- Want to protect the confidentiality of our data
- Data at Rest
    - Encryption of the data at rest is necessary!
        - Hard drive or per file encryption
        - Hardware based or software based
- Data in Transit
    - How are we protecting our data moving from point A to point B?
    - Link encryption and End to End Encryption
        - SSL, TLS, IPSec, AES, etc…
        - Encrypting the traffic as it moves is just as important as Data at Rest encryption/protection

Establish handling requirements

- As with physical assets, it is important that classified information assets are clearly marked and labeled

Record Retention and Disposal

- Strip-cut shredders—cut paper in long, thin strips
- Cross-cut shredders—preferable to strip-cut, these cut paper into small rectangular fragments
- Particle-cut shredders—similar to cross-cut; creates tiny square or circular fragments
- Hammermills—pound paper through a screen
- Granulators (or disintegrators)—repeatedly cut paper into fine, mesh-size particles

Security Levels

- Level 1—Least secure, cuts paper into 12-mm strips. Not suitable for classified information.
- Level 2—Cuts paper into 6-mm strips. Not suitable for classified information
- Level 3—Cuts paper into 2-mm strips. Limited suitability for confidential information.
- Level 4—Cuts paper into particles 2 × 15 mm particles. Suitable for Sensitive but Unclassified or Business Proprietary information.
- Level 5—Cuts paper into 0.8 × 12 mm particles. Suitable for Classified information.
- Level 6—Cuts paper into 0.8 × 4 mm particles. Suitable for Top Secret information.

Record Retention and Disposal

- Methods of destroying data contained on magnetic media include various techniques for *clearing* or *sanitizing* data
- *Erasure or reformatting*
  - Is it really gone?
- *Disk wiping*, or *overwriting*, is a method of writing over existing data—typically with a stream of zeroes, ones, or a random pattern of both

Record Retention and Disposal

- *Degaussing* is a technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.
- This is performed with a machine called a degausser, which applies a magnetic field to the media and then removes it, eliminating the residual magnetic signals on the media.

End of Domain 2!

- Classify information and supporting assets
- Determine and maintain ownership
- Protect Privacy
- Ensure appropriate retention
- Determine data security controls
- Establish handling requirements

CISSP

Domain 3

Security Engineering

(Engineering and Management of Security)

Key Areas

- Implement and manage an engineering lifecycle using security design principles
- Fundamental concepts of security models
- Controls and countermeasures based upon information systems security standards
- Security capabilities of information systems
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

Key Areas

- Vulnerabilities in Web-based systems
- Vulnerabilities in mobile systems
- Vulnerabilities in embedded devices and cyber-physical systems
- Cryptography
- Apply secure principles to site and facility design
- Facility security

Implement and manage an engineering lifecycle using security design principles

According to INCOSE (International Council on Systems Engineering)

- “Systems Engineering is an interdisciplinary approach and a means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem.”

Implement and manage an engineering lifecycle using security design principles

- Concept of Operations
- Requirements
- Design
- Implementation
- Test and Verify
- Validate
- Operation and Maintenance

Implement and manage an engineering lifecycle using security design principles

- NIST 800-14 five cycle planning phases
  - Initiation
  - Development and Acquisition
  - Implementation
  - Operation and Maintenance
  - Disposal

NIST 800-14 five cycle planning phases

- Initiation – During the initiation phase, the need for a system is expressed and the purpose of the system is documented.
- Development/ Acquisition – During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining the system.
- Implementation – During implementation, the system is tested and installed or fielded. Activities include installing/ turning on controls, security testing, certification, and accreditation.

NIST 800-14 five cycle planning phases

- Operation/ Maintenance – During this phase, the system performs its work. Typically, the system is also being modified by the addition of hardware and software and by numerous other events. Activities include security operations and administration, operational assurance, and audits and monitoring.
- Disposal – The disposal phase of the IT system lifecycle involves the disposition of information, hardware, and software. Activities include moving, archiving, discarding, or destroying information and sanitizing the media.

Fundamental concepts of security models

- Bell-LaPadula
- Biba
- Clark Wilson
- Chinese Wall/Brewer-Nash

Bell-LaPadula

- Originally developed for the U.S. Department of Defense.
- Focused on maintaining the confidentiality of objects.
  - Not allowing users at a lower security level to access objects at a higher security level.
- Simple Security Property: “no read up”: a subject at a specific classification level cannot read an object at a higher classification level. Subjects with a Secret clearance cannot access Top Secret objects, for example.
- Security Property: “no write down”: a subject at a higher classification level cannot write to a lower classification level. For example, subjects who are logged into a Top Secret system cannot send emails to a Secret system.

Biba

- Integrity Model
- Simple Integrity Axiom: “no read down”: a subject at a specific classification level cannot read data at a lower classification. This prevents subjects from accessing information at a lower integrity level. This protects integrity by preventing bad information from moving up from lower integrity levels.
- Integrity Axiom: “no write up”: a subject at a specific classification level cannot write data to a higher classification. This prevents subjects from passing information up to a higher integrity level than they have clearance to change. This protects integrity by preventing bad information from moving up to higher integrity levels.

Clark Wilson

- Real-world integrity model that protects integrity by requiring subjects to access objects via programs.
- Because the programs have specific limitations to what they can and cannot do to objects, this model effectively limits the capabilities of the subject.
- Uses two primary concepts to ensure that security policy is enforced: well-formed transactions and separation of duties.

Chinese Wall/Brewer-Nash

- The Chinese Wall model is designed to avoid conflicts of interest by prohibiting one person, such as a consultant, from accessing multiple conflict of interest categories

Controls and countermeasures based upon information systems security standards

- Evaluation methods and criteria are designed to gauge the real-world security of systems and products.

- The Orange Book / Trusted Computer System Evaluation Criteria
- ITSEC – Information Technology Security Evaluation Criteria
- Common Criteria
- PCI-DSS

The Orange Book / Trusted Computer System Evaluation Criteria

- D: Minimal protection. This division describes TCSEC-evaluated systems that do not meet the requirements of higher divisions (C through A). • C: Discretionary protection. "Discretionary" means discretionary access control systems (DAC). • B: Mandatory protection. "Mandatory" means mandatory access control systems (MAC). • A: Verified protection. Includes all requirements of B, plus additional controls.

ITSEC – Information Technology Security Evaluation Criteria

- Refers to TCSEC Orange Book levels, separating functionality (F, how well a system works) from assurance (the ability to evaluate the security of a system).
- There are two types of assurance: effectiveness and correctness
- Assurance correctness ratings range from E0 (inadequate) to E6 (formal model of security policy);
- Functionality ratings range include TCSEC equivalent ratings (F-C1, F-C2, etc.).

Common Criteria

- The International Common Criteria is an internationally agreed upon standard for describing and testing the security of IT products. It presents a hierarchy of requirements for a range of classifications and systems
- Within the Common Criteria, there are seven EALs, each building upon the previous level. Example, EAL4-rated products can be expected to meet or exceed the requirements of products rated EAL1, EAL2 or EAL3.

The common criteria levels

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested, and reviewed
- EAL5: Semi-formally designed and tested
- EAL6: Semi-formally verified, designed, and tested
- EAL7: Formally verified, designed, and tested

Common Criteria Terms

- Target of Evaluation (ToE): the system or product that is being evaluated
- Security Target (ST): the documentation describing the TOE, including the security requirements and operational environment
- Protection Profile (PP): an independent set of security requirements and objectives for a specific category of products or systems, such as firewalls or intrusion detection systems
- Evaluation Assurance Level (EAL): the evaluation score of the tested product or system

PCI-DSS

- The Payment Card Industry Data Security Standard (PCI-DSS) is a security standard created by the Payment Card Industry Security Standards Council (PCI-SSC).
- The council is comprised of American Express, Discover, Master Card, Visa, and others.
- PCI-DSS seeks to protect credit cards by requiring vendors using them to take specific security precautions

Security capabilities of information systems

- Hardware Segmentation
  - Hardware segmentation takes process isolation one step further by mapping processes to specific memory locations. This provides more security than (logical) process isolation alone.
- Memory Protection
  - Memory protection prevents one process from affecting the confidentiality, integrity, or availability of another. This is a requirement for secure multiuser (more than one user logged in simultaneously) and multitasking (more than one process running simultaneously) systems

Security capabilities of information systems

- Process isolation
  - A logical control that attempts to prevent one process from interfering with another.
  - Common feature among multiuser operating systems such as Linux, UNIX, or recent Microsoft Windows operating systems.
  - Older operating systems such as MS-DOS provide no process isolation.
    - No process isolation means a crash in any MS-DOS application could crash the entire system.

Security capabilities of information systems

- Reference Monitor
    - A core function of the kernel is running the reference monitor, which mediates all access between subjects and objects. It enforces the system's security policy, such as preventing a normal user from writing to a restricted file, such as the system password file.
- Virtualization
    - Virtualization adds a software layer between an operating system and the underlying computer hardware. Allows multiple guest operating systems or VMs to run simultaneously on one physical or host computer.

Security capabilities of information systems

- Constrained User Interface
  - Limiting what the users sees on a screen or display by using data views or certain menus for the user
- Fault Tolerance
  - For systems within an organization to be able to continually provide operational availability, they must be implemented with fault tolerance in mind.
- Trusted Platform Module
  - Hardware module for data encryption. On most if not all mother boards on modern computers.

Coming Up!

- Next we will continue one with Domain 3 starting with Assessing and Mitigating the Vulnerabilities of Security Architectures, Designs and Solution Elements.

*

Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based
- Server-based
- Database security
- Large scale parallel data systems
- Distributed systems
- Cryptographic systems

Client Based

Desktops and Laptops

- A supported and licensed operating system is running
- Updated, verified, and supported anti-malware and anti-virus capabilities are installed
- A host-based intrusion detection system is installed. The whole drive or sensitive information on the drive is encrypted with strong encryption
- Whenever possible, the client operates in a limited account that does not have administrative privileges
- Whenever possible, the client system is part of a continuous monitoring program that monitors for vulnerabilities and patches them when needed without the need for interaction of the end-user
- Changes to the operating system or new software are validated through an assessment process to determine any security impacts.

Server-Based

- Servers are popular targets for attackers
- How can we protect them?
  - Physical Locations
  - Access Control
  - Patch management
  - Network Segregation
  - Maintain Dataflows

Server-Based

Data Flow Control

- Controls between the various components that enforce the data flow to only the required recipients and how the communication is protected if required
- The concept of least privilege should be employed to ensure data only flows to authorized recipients and processes.

Database Security

- Inference
- Aggregation
- Data Mining
- Data Analytics
- Warehousing

Inference

- Ability to deduce (infer) sensitive or restricted information from observing available information
- Users may be able to determine unauthorized information from what information they can access and may never need to directly access unauthorized data
- One of the hardest threats to control
- Get to know the processes; spend the necessary time with Data/ Business Owners

Aggregation

- Is combining non-sensitive data from separate sources to create sensitive information.

- We need to understand the fields and types of information present in a database.
- We also need to understand the possible combinations of information including which combinations may result in an escalation of sensitivity.

Warehousing

- Repository for information collected from a variety of data sources.
- The data stored in a data warehouse is not used for operational tasks but rather for analytical purposes.
- The data warehouse combines all of the data from various databases into one large data container.

Data Mining/Data Analytics

- Discovering information in data warehouses by running queries on the data
- A large repository of data is required to perform data mining
- Used to reveal hidden relationships, patterns, and trends in the data warehouse
- Based on a series of analytical techniques taken from the fields of mathematics, statistics, cybernetics, and genetics.

Large-scale Parallel Data Systems

- Parallel Data systems take large amounts of information and break up the processing to separate systems
  - Spreading the love around
  - Makes processing much more efficient and faster

- Vulnerabilities are shared by the entire system

Distributed Systems

- Cloud computing outsources IT infrastructure, storage, or applications to a third-party provider.
- Implies geographic diversity of computer resources
- Goal of cloud computing is to allow large providers to leverage their economies of scale to provide computing resources to other companies that typically pay for these services based on their usage

Cloud Computing

- SaaS – Software as a Service
  - Using Applications, OS and Apps already there
    - Web Mail; Office 365
- PaaS – Platform as a Service
  - Configured services
    - Web Hosting
- IaaS – Infrastructure as a Service
  - Virtualized Operating System
    - Server Hosting

Distributed Systems

- Grid computing represents a distributed computing approach that attempts to achieve high computational performance by a nontraditional means.
- Grid computing attempts to harness the computational resources of a large number of dissimilar devices

Distributed Systems

- Peer-to-peer (P2P) networks alter the classic client/ server computer model
- Any system may act as a client, a server, or both, depending on the data needs
- Decentralized peer-to-peer networks are resilient: there are no central servers that can be taken offline

Cryptographic Systems

- There are three primary types of modern encryption: symmetric, asymmetric, and hashing.
- Symmetric encryption uses one key: the same key encrypts and decrypts
- Asymmetric cryptography uses two keys: if you encrypt with one key, you may decrypt with the other
- Hashing is a one-way cryptographic transformation using an algorithm

ICS – Industrial Control Systems

- SCADA – Supervisory Control and Data Acquisition systems
  - assembly of interconnected equipment used to monitor and control physical equipment in industrial environments.

- Threats
  - DoS Attacks
  - Unauthorized Access
  - Human Error
  - Attacks on end systems or office networks
  - Unauthorized Remote Access

Vulnerabilities in Web-based systems

- XML - Extensible Markup Language
  - Markup language designed as a standard way to encode documents and data.
  - Similar to, but more universal than, HTML.
  - Used on the Web, but is not tied to it.
  - Can be used to store application configuration, output from auditing tools, and many other uses.
  - Extensible means users may use XML to define their own data formats.
- SAML - Security Assertion Markup Language
  - An XML-based framework for exchanging security information, including authentication data. One goal of SAML is to enable Web single-sign on (SSO) at an Internet scale.

Vulnerabilities in Web-based systems

- Java
  - Object-oriented language used not only to write applets but also as a general-purpose programming language. Java bytecode is platform-independent: it is interpreted by the Java virtual machine (JVM).
  - Run in a sandbox, which segregates the code from the operating system. The sandbox is designed to prevent an attacker who is able to compromise a java applet from accessing system files, such as the password file.
- ActiveX
  - Controls are the functional equivalent of Java applets. They use digital certificates instead of a sandbox to provide security. Unlike Java, ActiveX is a Microsoft technology that works on Microsoft Windows operating systems only

OWASP - Open Web Application Security Project

- Represents one of the best application security resources. OWASP provides a tremendous number of free resources dedicated to improving organizations' application security posture
- One of their best-known projects is the OWASP Top 10 project, which provides guidance on what are considered to be the ten most significant application security risks

Vulnerabilities and Defense in Mobile Systems

- Defenses include policy administrative controls such as restricting the use of mobile devices via policy.
- Technical controls to mitigate infected mobile computers include requiring authentication at OSI model layer 2 via 802.1X. 802.1X authentication may be bundled with additional security functionality, such as verification of current patches and antivirus signatures.

Vulnerabilities and Defense in Mobile Systems

- Another mobile device security concern is the loss or theft of a mobile device, which threatens confidentiality, integrity, and availability of the device and the data that resides on it. Backups can assure the availability and integrity of mobile data.
- Full disk encryption (also known as whole disk encryption) should be used to ensure the confidentiality of mobile device data.
- Remote wipe capability is another critical control, which describes the ability to erase (and sometimes disable) a mobile device that is lost or stolen.

Vulnerabilities in embedded devices

- Embedded devices are devices that are small form factor, not very powerful but still need to run a "watered down" OS.
- Usually perform specific tasks and not full blow systems like your desktop/laptop
  - Wireless Routers
  - Mobile Devices (cell phones/tablets)
  - Media Players

Coming Up!

- Next we will continue on with Domain 3 starting with Cryptography.

*

Cryptography

- Cryptographic lifecycle
- Cryptographic types
- Public key infrastructure
- Key management practices
- Digital signatures
- Digital rights management
- Non-repudiation
- Integrity
- Methods of cryptanalytic attacks

Cryptographic lifecycle

- As great as Cryptography is, it does have a shelf life.
- Faster processors, types of software/hardware developed, more vulnerabilities
- Strong, Weak, Compromised
- When do we know it is “no good” anymore?
    - Hashes
        - When we have collisions (hashes are the same)
        - When we can have a side channel attack
    - Encryption
        - When we can get information without the key within a reasonable timeframe
        - When data is accessed by unauthorized people

Cryptographic Types

- Symmetric
- Asymmetric

Symmetric Cryptography

- Symmetric algorithms operate with a single cryptographic key that is used for both encryption and decryption of the message.
- Single Key; Shared Key; Private Key; Secret Key
- Key management is a challenge
  - Keeping it secure; sharing it with authorized individuals
- Fast and cheap to implement

Symmetric Cryptography Examples

- DES
- 3DES
- AES
- IDEA
- SAFER
- CAST
- Blowfish
- Two Fish
- RC4 and RC5

Asymmetric Cryptography

- Newer than Symmetric
- 2 Keys; Public and Private; Key Pairs
    - One to encrypt; Other to decrypt

- RSA
- El Gamal
- ECC – Elliptic Curves (strongest, good for wireless and smart cards)
- Diffie-Helman

Hybrid Cryptography

- Mixing the best of both worlds
- Symmetric and Asymmetric

PKI - Public Key Infrastructure

- Leverages all three forms of encryption to provide and manage digital certificates.
- A digital certificate is a public key signed with a digital signature.
- Digital certificates may be server based or client based. If the two are used together, they provide mutual authentication and encryption.
- The standard digital certificate format is X. 509

PKI - Public Key Infrastructure

- Digital certificates are issued by Certificate Authorities (CAs). Registration Authorities (RAs) authenticate the identity of a certificate holder before issuing a certificate to them. An organization may act as a CA or RA or both
- Certificate Revocation List – CRL
  - A certificate may be revoked if the private key has been stolen, an employee is terminated, etc. A CRL is a flat file and does not scale well.
  - The Online Certificate Status Protocol (OSCP) is a replacement for CRLs and uses client-server design that scales better

Key Management

- Certificate Authorities issue digital certificates and distribute them to certificate holders.
- The confidentiality and integrity of the holder's private key must be assured during the distribution process. Public/ private key pairs used in PKI should be stored centrally and securely
- Users may lose their private key as easily as they may forget their password. A lost private key that is not securely stored means that anything encrypted with the matching public key will be lost

Digital Signatures

- Used to cryptographically sign documents
- Provide nonrepudiation, which includes authentication of the identity of the signer, and proof of the document's integrity
- This means the sender cannot later deny signing the document.

- Uses Hashes to determine

Digital Rights Management

- Control and protection to content providers over their own digital media.
- From the content's point of view, there are three key components to its lifecycle
  - Creation of content
  - Distribution and upkeep of content
  - Use of content

Digital Rights Management

- Always-On DRM
  - Have to be on the Internet to access
- USB Key
  - If you have the “key” you can read the data
  - Data can be on anyones/everyones computer
- Digital Watermark
  - Was for printed material
  - Can be on Audio/Video as well

Non-Repudiation

- Nonrepudiation means a user cannot deny (repudiate) having performed a transaction.
- It combines authentication and integrity: nonrepudiation authenticates the identity of a user who performs a transaction and ensures the integrity of that transaction.

Integrity

- A hash function provides encryption using an algorithm and no key.
- They are called "one-way hash functions" because there is no way to reverse the encryption.
- A variable-length plaintext is hashed into a fixed-length hash value, often called a message digest or simply a hash.
- Hash functions are primarily used to provide integrity: if the hash of a plaintext changes, the plaintext itself has changed
  - SHA – Secure Hashing Algorithm
  - MD5 – Message Digest
  - HAVAL – Hash of Variable Length

Crypto Attacks

- Brute Force
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Known Key
- Side-Channel Attack

Brute Force

- A brute-force attack generates the entire keyspace, which is every possible key. Given enough time, the plaintext will be recovered.

Known Plaintext

- Relies on recovering and analyzing a matching plaintext and ciphertext pair
  - Goal is to derive the key that was used.
- Why do you need the key if you already have the plaintext?
  - Recovering the key would allow you to decrypt other ciphertexts encrypted with the same key.

Chosen Plaintext

- A cryptanalyst chooses the plaintext to be encrypted in a chosen plaintext attack
    - Goal is to derive the key
- Encrypting without knowing the key is done via an “encryption oracle” or a device that encrypts without revealing the key.

Chosen Ciphertext

- Mirror chosen plaintext attacks
  - Difference being that the cryptanalyst chooses the ciphertext to be decrypted
- This attack is usually launched against asymmetric cryptosystems, where the cryptanalyst may choose public documents to decrypt that are signed (encrypted) with a user's public key.

Known Key

- The cryptanalyst knows something about the key, to reduce the efforts used to attack it.
- If the cryptanalyst knows that the key is an uppercase letter and a number only, other characters may be omitted in the attack

Side-Channel

- Use physical data to break a cryptosystem, such as monitoring CPU cycles or power consumption used while encrypting or decrypting.

Coming Up!

- Next we will wrap up Domain 3 by first looking at Secure Principles to Site and Facility Design

Apply Secure Principles to Site and Facility Design

Few things as an Security Professional we need to do

- Security Survey
  - Threats, Assets, Policies, Procedures
- Vulnerability Assessment

Apply Secure Principles to Site and Facility Design – American Institute of Architects

- Facility security control during and after hours of operation
- Personnel and contract security policies and procedures
- Personnel screening
- Site and building access control
- Video surveillance, assessment, and archiving
- Natural surveillance opportunities
- Protocols for responding to internal and external security incidents
- Degree of integration of security and other building systems
- Shipping and receiving security
- Property identification and tracking
- Proprietary information security
- Computer network security
- Workplace violence prevention
- Mail screening operations, procedures, and recommendations
- Parking lot and site security
- Data center security
- Communications security
- Executive protection
- Business continuity planning and evacuation procedure

Design and Implement Physical Security

- Wiring Closets and Server Rooms
  - Entrances; Lighting Protection (Grounding); Access Control; Rack Security; HVAC
- Media Storage
- Evidence Storage
  - Faraday bag
- Restricted Areas
- Data Center
  - Proximity cards, man traps

Design and Implement Physical Security

- Utilities and HVAC Considerations
  - Generators, UPS, Humidity Control
- Water Issues
  - Flooding, leaks
- Fire Prevention, Detection and Suppression

Fire Prevention, Detection and Suppression

- **Wet Systems** – Have a constant supply of water in them at all times; once activated, these sprinklers will not shut off until the water source is shut off.
- **Dry Systems**– Do not have water in them. The valve will not release until the electric valve is stimulated by excess heat
- **Pre-Action Systems** – Incorporate a detection system, which can eliminate concerns of water damage due to false activations. Water is held back until detectors in the area are activated.
- **Deluge Systems** – Operate in the same function as the pre-action system except all sprinkler heads are in the open position.

Domain 3 Complete!

- Implement and manage an engineering lifecycle using security design principles
- Fundamental concepts of security models
- Controls and countermeasures based upon information systems security standards
- Security capabilities of information systems
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

Domain 3 Complete!

- Vulnerabilities in Web-based systems
- Vulnerabilities in mobile systems
- Vulnerabilities in embedded devices and cyber-physical systems
- Cryptography
- Apply secure principles to site and facility design
- Facility security

*

CISSP

Domain 4

Communication and Network Security

(Designing and Protecting Network Security)

Key Areas

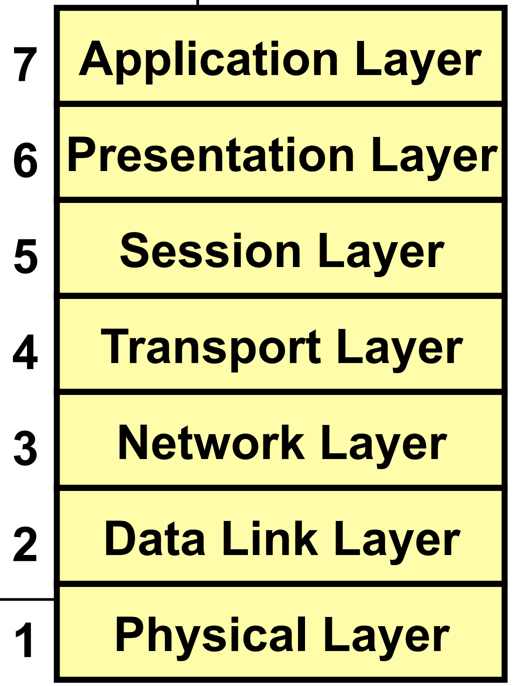
- Apply Secure Design Principles to network Architecture
- Securing network components
- Secure communication channels
- Prevent or mitigate network attacks

Apply Secure Design Principles to network Architecture

- OSI and TCP/ IP models
- IP networking
- Implications of multilayer protocols (e.g., DNP3)
- Converged protocols (e.g., FCoE, MPLS, VoIP, iSCI)
- Software-defined networks
- Wireless networks
- Cryptography used to maintain communications security

The OSI Model

The OSI (Open Systems Interconnection) model uses a layered architecture to standardize the levels of service and the interaction types for networked computers.



7 Application Layer

6 Presentation Layer

5 Session Layer

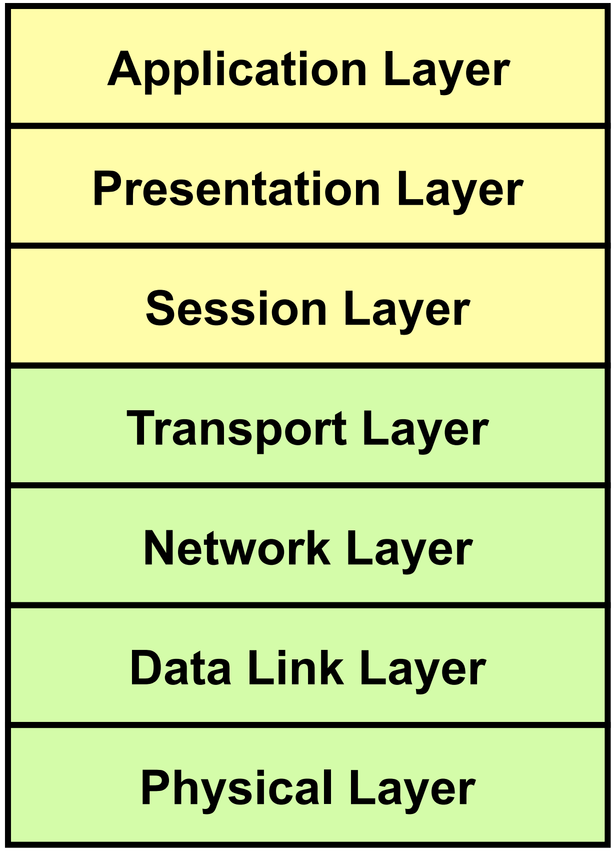
4 Transport Layer

3 Network Layer

2 Data Link Layer

1 Physical Layer

The OSI Model



Application Layer

Presentation Layer

Session Layer

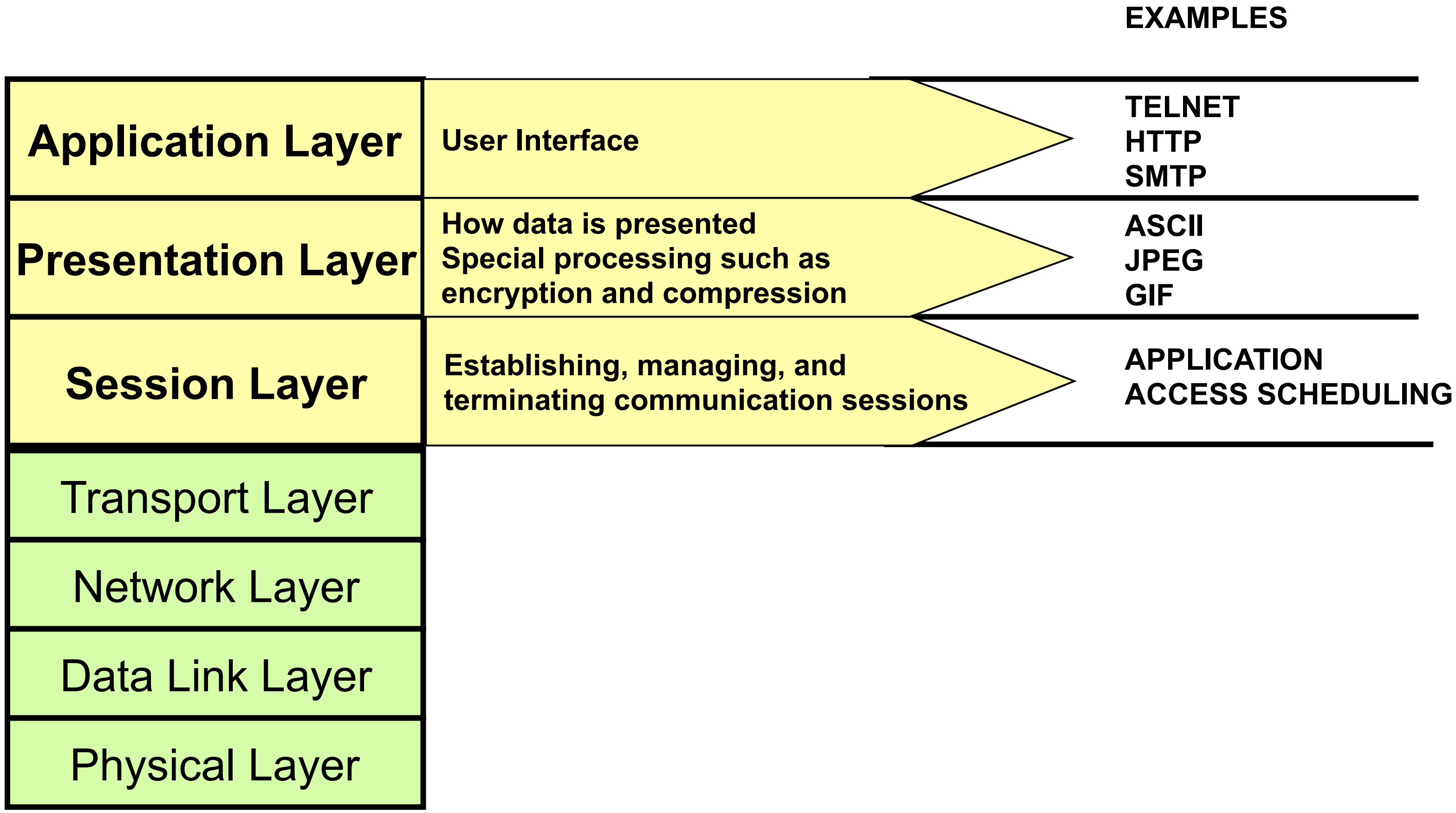
Transport Layer

Network Layer

Data Link Layer

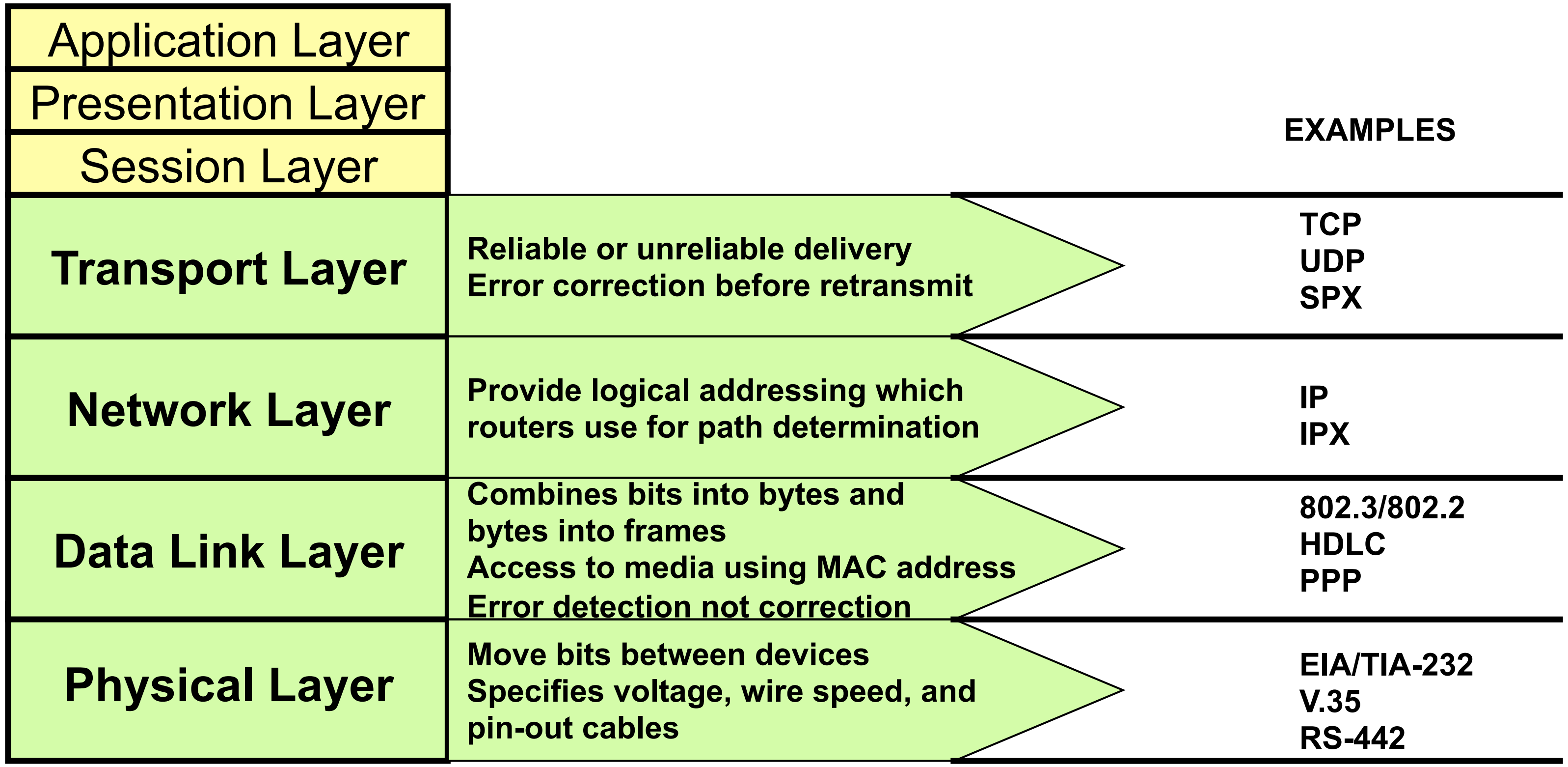
Physical Layer

The OSI Model Upper Layers



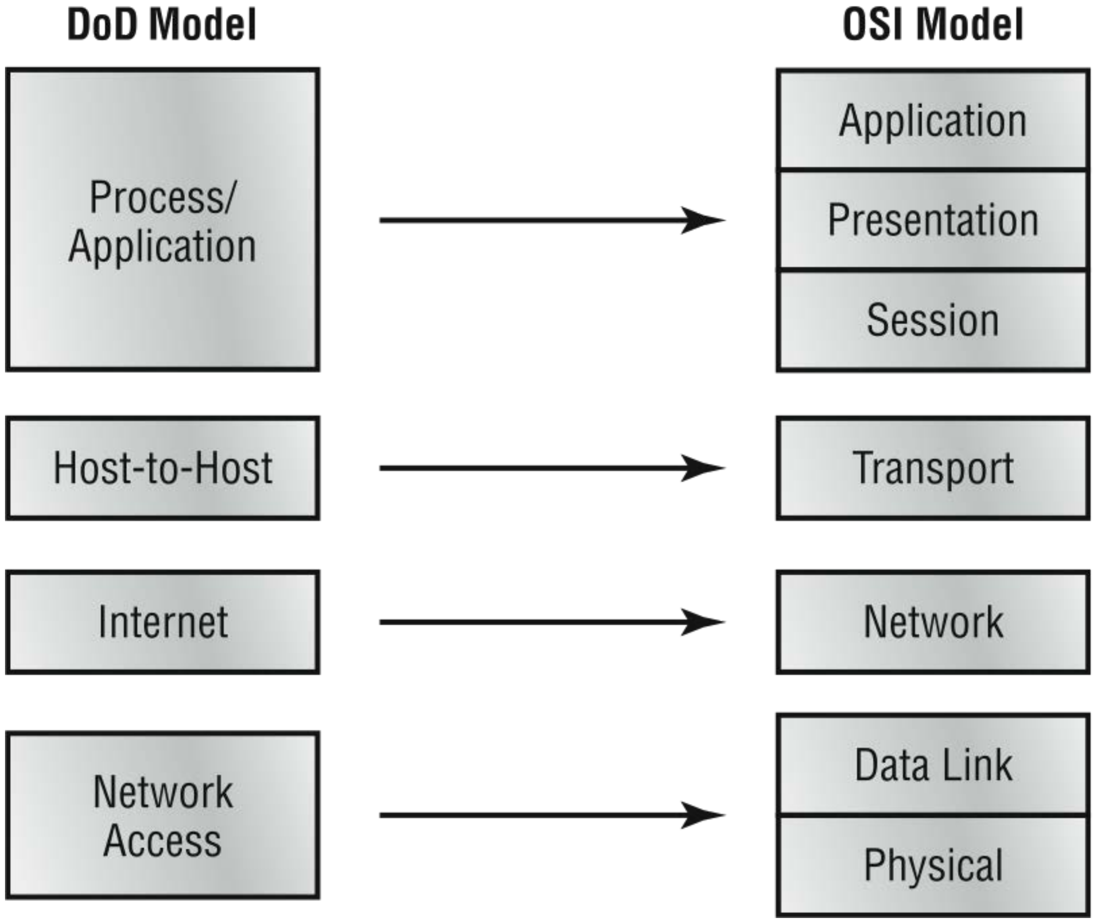
		EXAMPLES
Application Layer	User Interface	TELNET HTTP SMTP
Presentation Layer	How data is presented Special processing such as encryption and compression	ASCII JPEG GIF
Session Layer	Establishing, managing, and terminating communication sessions	APPLICATION ACCESS SCHEDULING
Transport Layer		
Network Layer		
Data Link Layer		
Physical Layer		

The OSI Model Lower Layers



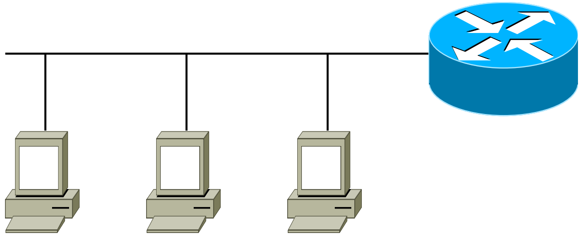
		EXAMPLES
Application Layer		
Presentation Layer		
Session Layer		
Transport Layer	Reliable or unreliable delivery Error correction before retransmit	TCP UDP SPX
Network Layer	Provide logical addressing which routers use for path determination	IP IPX
Data Link Layer	Combines bits into bytes and bytes into frames Access to media using MAC address Error detection not correction	802.3/802.2 HDLC PPP
Physical Layer	Move bits between devices Specifies voltage, wire speed, and pin-out cables	EIA/TIA-232 V.35 RS-442

TCP/IP Model

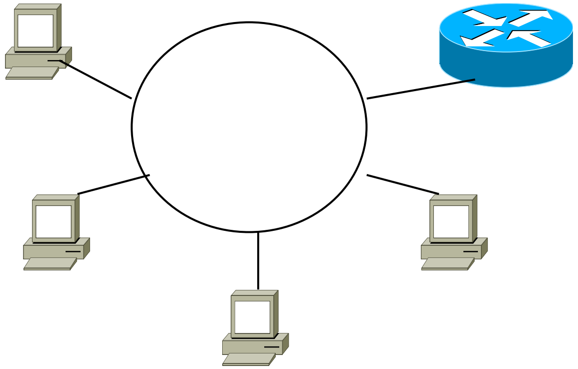

DoD Model
OSI Model
Process/ Application
Application
Presentation
Session
Host-to-Host
Transport
Internet
Network
Network Access
Data Link
Physical

Local Area Network (LAN)

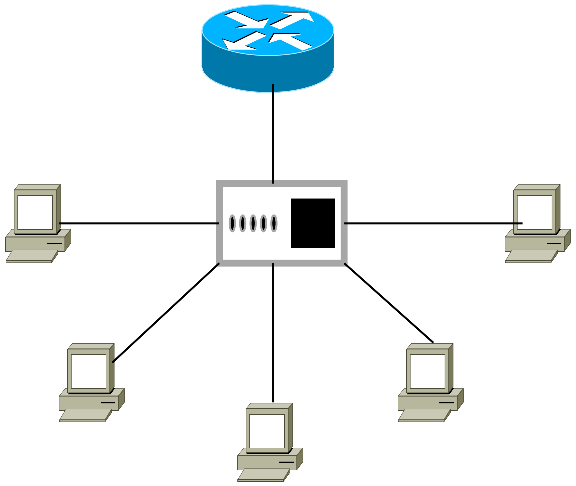
BUS Topology



RING Topology



STAR Topology



IP Networking

- Internet protocol (IP) is responsible for sending packets from the source to the destination hosts.
- Being an unreliable protocol, it does not guarantee that packets arrive error free or in the correct order
  - We have other protocols that help us out with delivery
- IP is responsible for showing the way for the data

IP Addressing

- IPv4
  - 32 bit values that uniquely identifies a system on a network
    - 192.168.100.100
  - 4 areas, octets, separated by decimals
    - Each octet is 8 bits (4 x 8 = 32 bits)

  - 0 – 255 range in each octet
    - 0.0.0.0 lowest
    - 255.255.255.255 highest

  - Broken up into Network and Host sections
    - Subnet Mask's job

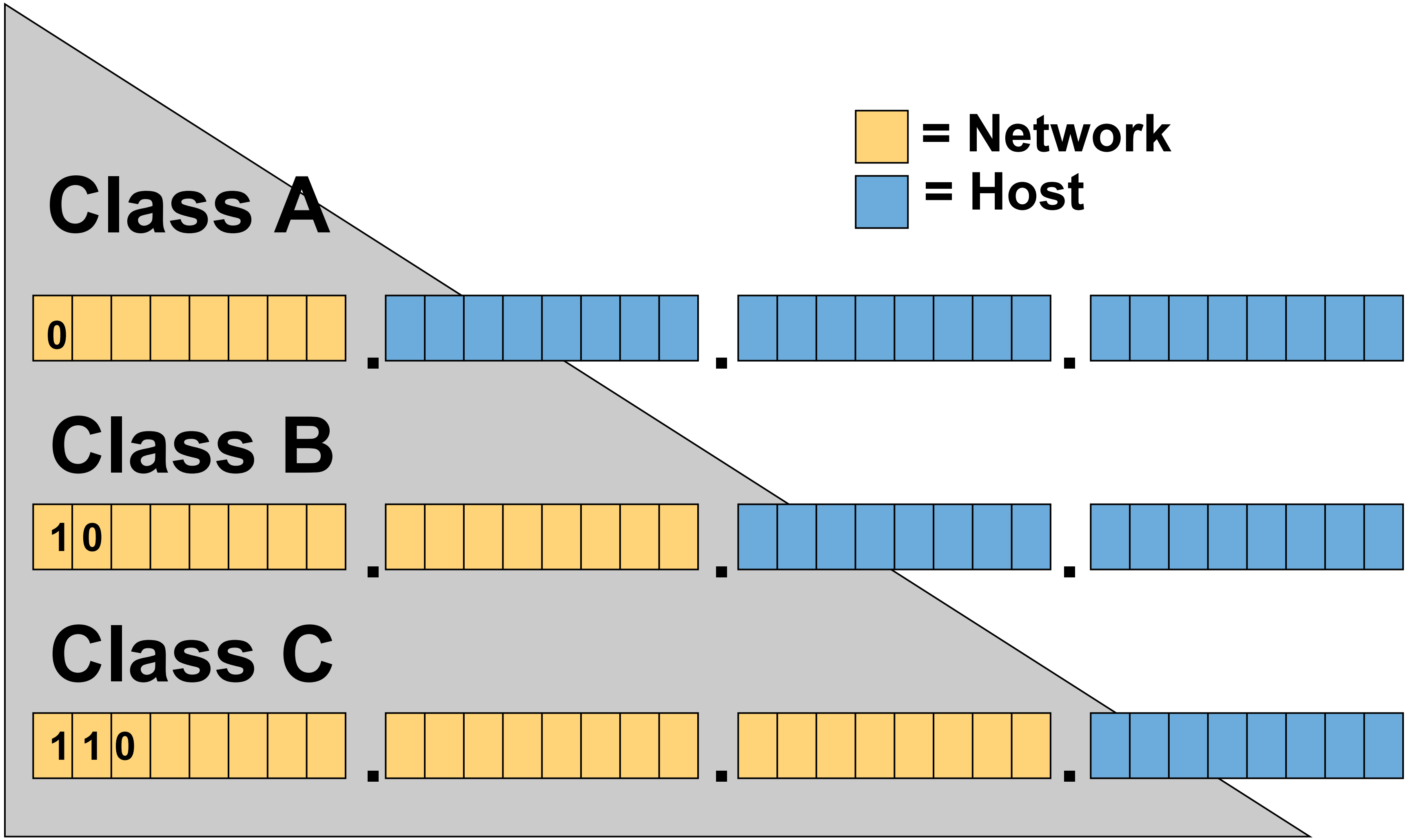
IP Addressing

- Subnet Mask
  - Responsible for covering up the networking portion of an IP address
    - Part you cannot change
  - Use to determine network range
    - Starting and ending addresses along with usable range
  - 0 – 255 range in each octet
    - 0.0.0.0 lowest
    - 255.255.255.255 highest

IP Addressing

- Default Gateway
  - Way out of your network
    - The gateway for the castle
  - When you have traffic destined for another network, then it has to travel through the Default Gateway
  - Network admins configure a Default Gateway

Classes of Addresses



🟨 = Network

🟦 = Host

Class A

0

Class B

1 0

Class C

1 1 0

Classes of Addresses

- Class A
    - 1 - 127
- Class B
    - 128 - 191
- Class C
    - 192 - 223
- Class D
    - Multicasting Addressing
    - 224 - 239
- Class E
    - Experimental Addressing
    - 240 - 254

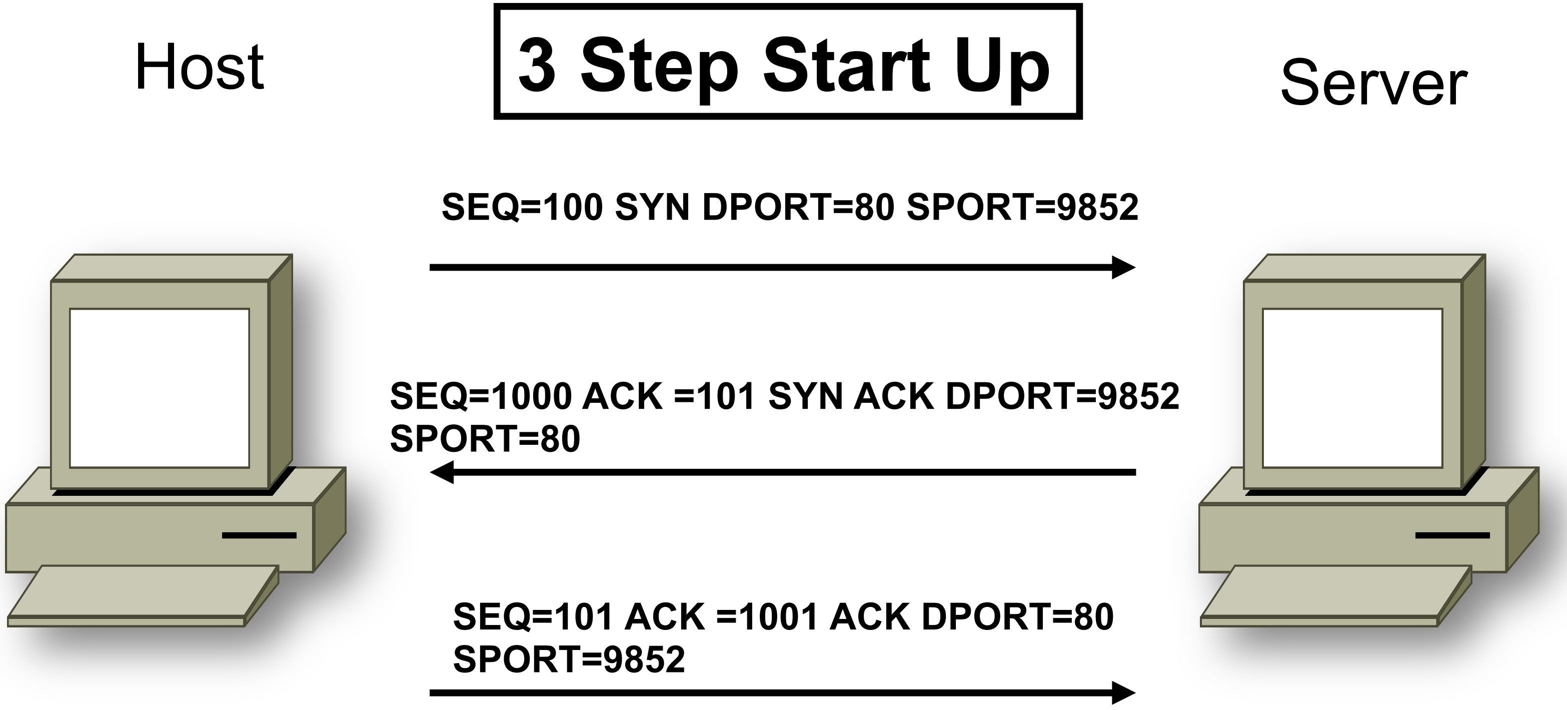
Special Addresses

- Private Addressing
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

- Loop Back
  - 127.0.0.0 – 127.255.255.255

TCP/IP Protocols

- TCP
  - Responsible for delivering your data
  - Reliable; Connection Oriented
  - Layer 4
  - 3 way handshake
    - SYN, ACK/SYN, ACK



Host

3 Step Start Up

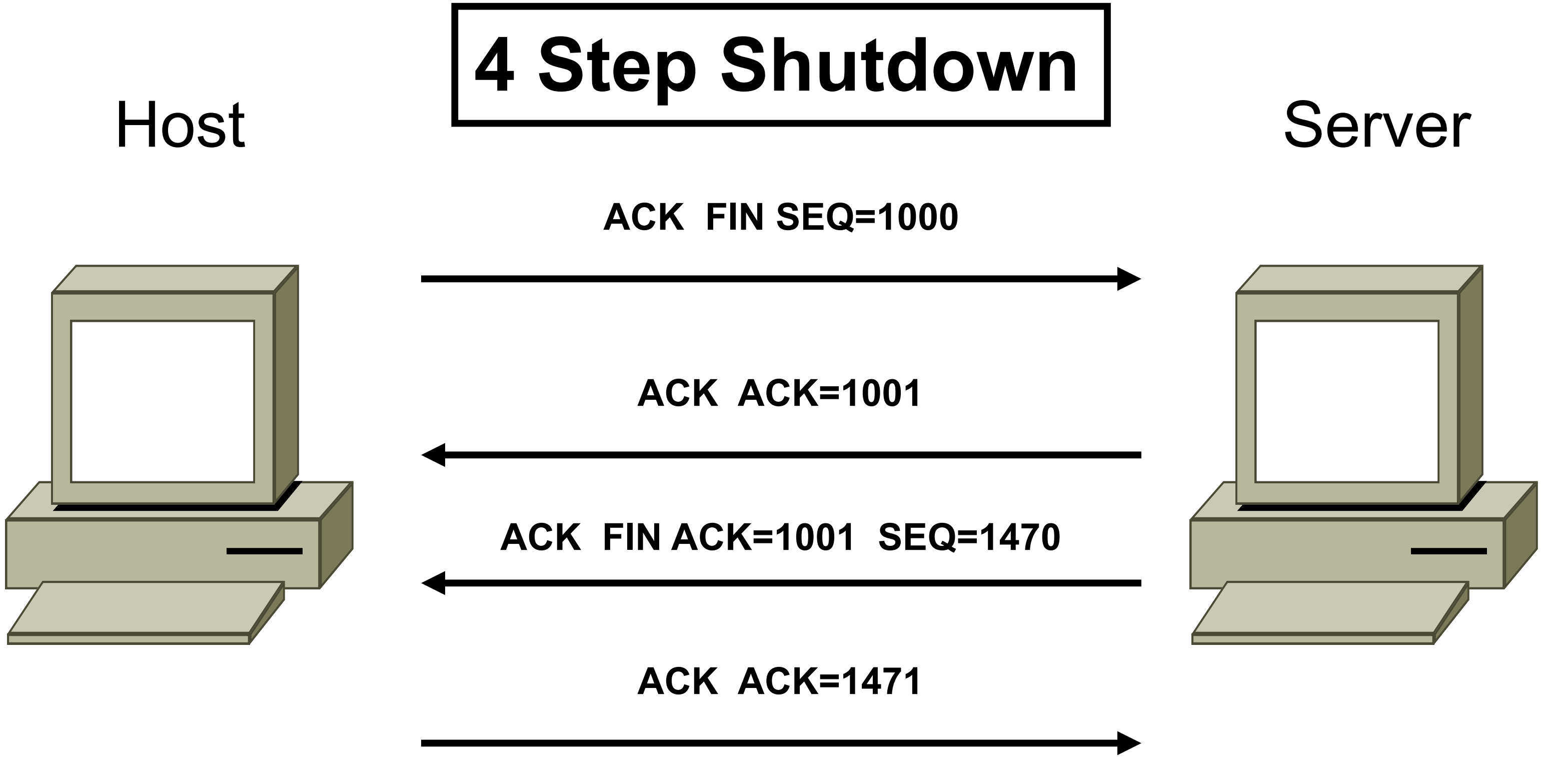
Server

SEQ=100 SYN DPORT=80 SPORT=9852

SEQ=1000 ACK =101 SYN ACK DPORT=9852 SPORT=80

SEQ=101 ACK =1001 ACK DPORT=80 SPORT=9852

Shutdown



4 Step Shutdown

Host

Server

ACK FIN SEQ=1000

ACK ACK=1001

ACK FIN ACK=1001 SEQ=1470

ACK ACK=1471

Ports

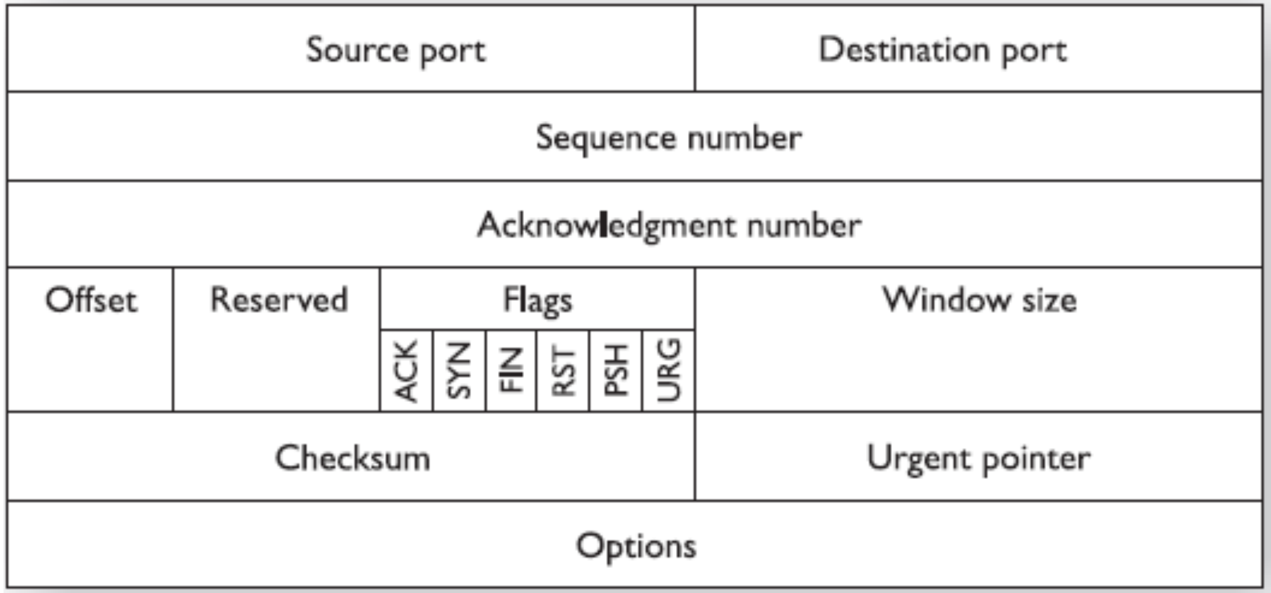
- Ports are like doors into and out of your system
- Well-Known Ports – Ports 0 through 1023 are considered to be well known. Ports in this range are assigned by IANA and, on most systems, can only be used by privileged processes and users
- Registered Ports – Ports 1024 through 49151 can be registered with IANA by application developers but are not assigned by them. The reason for choosing a registered instead of a well- known port can be that on most systems, the user may not have the privileges to run an application on a well-known port
- Dynamic or Private Ports – Ports 49152 through 65535 can be freely used by applications

TCP Flags

- SYN – Synchronize Flags; Usually at the beginning of a communication
- ACK – Acknowledgement
- PSH – Push, forces data
- URG – Urgent, specifies the data packet is urgent
- FIN – Finish, how to finalize or end a connection
- RST – Reset, ends TCP without notice, not nicely like a FIN

TCP Header

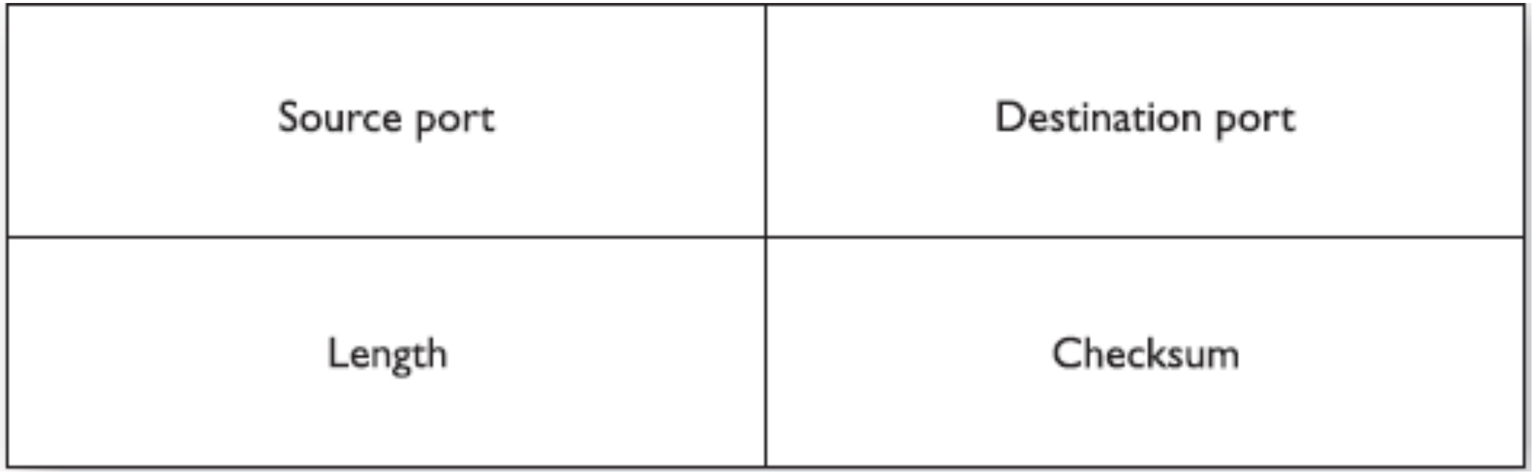
- First thing read from a packet
- Important information for the data
  - Where it’s going, Where it’s been, Sequence, Acknowledgement



<table>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgment number</td></tr>
<tr><td rowspan="2">Offset</td><td rowspan="2">Reserved</td><td colspan="6">Flags</td><td rowspan="2">Window size</td></tr>
<tr><td>ACK</td><td>SYN</td><td>FIN</td><td>RST</td><td>PSH</td><td>URG</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="9">Options</td></tr>
</table>

UDP – User Datagram Protocol

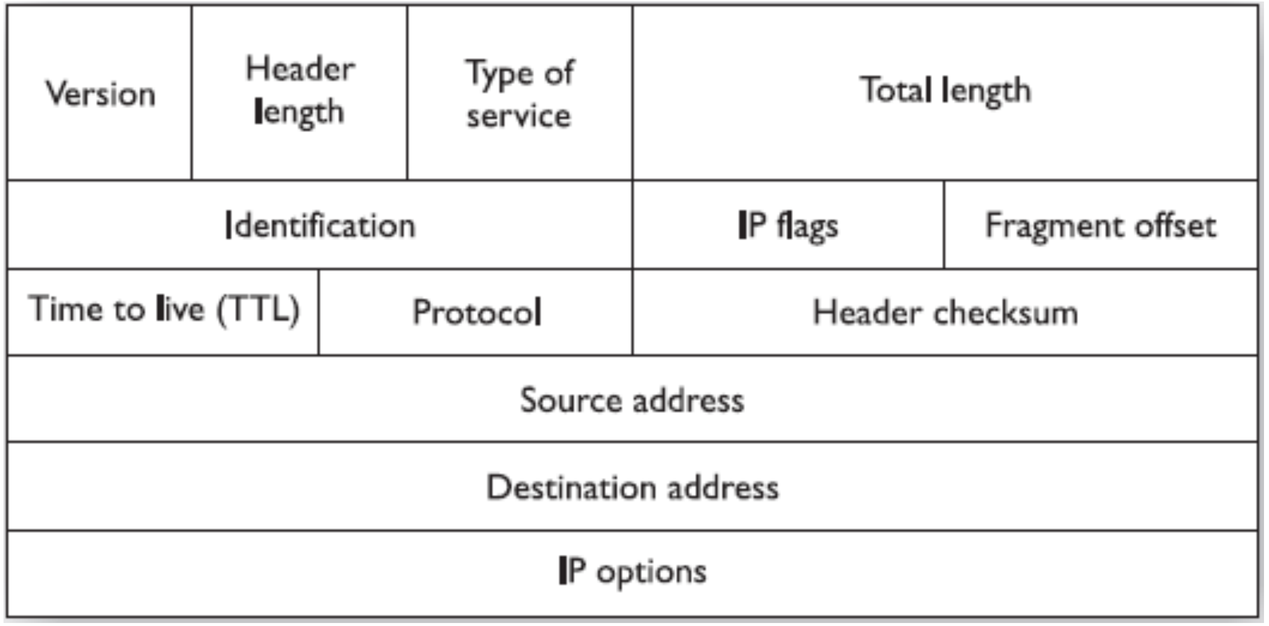
- Unreliable; Best Effort Protocol; Connectionless
- Smaller header than TCP
- Layer 4



Source port	Destination port
Length	Checksum

IP – Internet Protocol

- Provides addressing for packet delivery
  - Don’t get confused with TCP for delivery, IP only shows the way
- Logical addressing and routing
- Layer 3

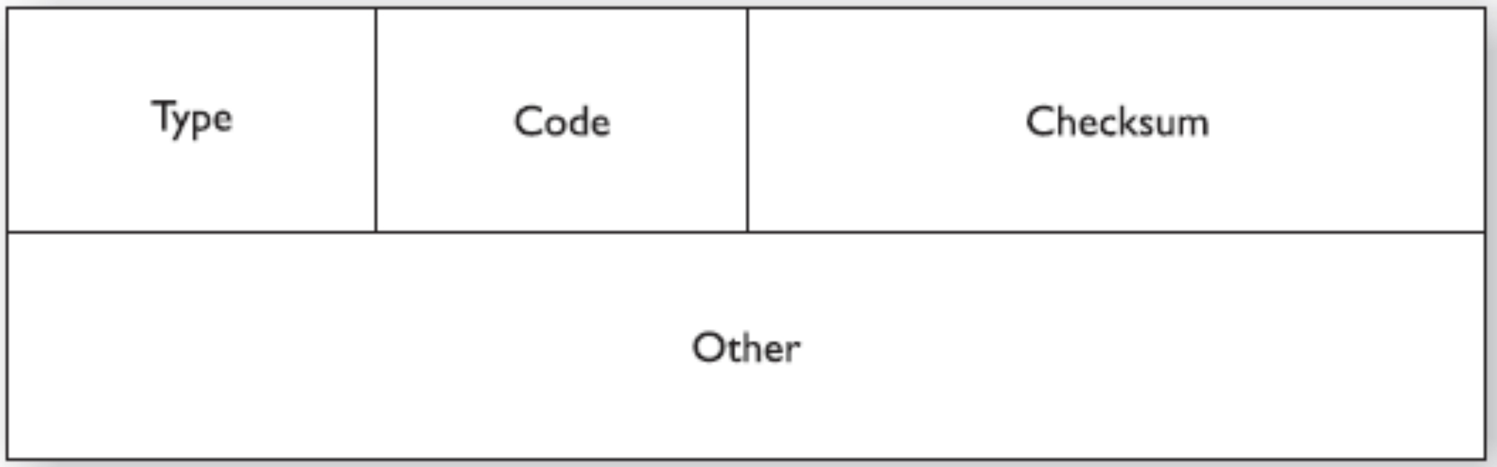


<table>
<tr><td>Version</td><td colspan="2">Header length</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="4">Identification</td><td>IP flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live (TTL)</td><td colspan="2">Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="6">Source address</td></tr>
<tr><td colspan="6">Destination address</td></tr>
<tr><td colspan="6">IP options</td></tr>
</table>

ICMP – Internet Control Messaging Protocol

- How we get status information
  - “Destination cannot be reached”

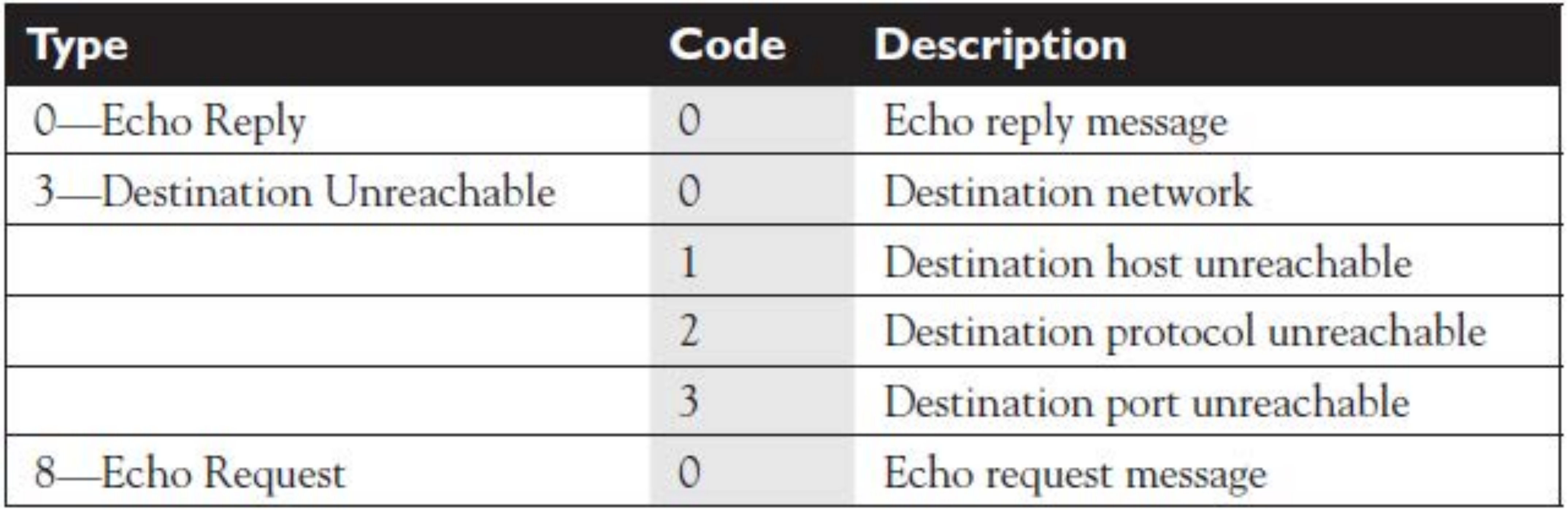
- Ping and Tracert



Type	Code	Checksum
Other		

ICMP – Internet Control Messaging Protocol

- ICMP Types and Codes



Type	Code	Description
0—Echo Reply	0	Echo reply message
3—Destination Unreachable	0	Destination network
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
8—Echo Request	0	Echo request message

ARP – Address Resolution Protocol

- IP to MAC Address

- We usually have the Logical address (IP) and we need the hardware address (MAC) to deliver the information.

Application Layer Protocols

- HTTP/HTTPS
- DNS
- SMTP
- POP3
- IMAP4
- SNMP
- FTP
- TFTP
- SFTP
- Telnet
- SSSH
- SCP
- NTP
- LDAP

NetBIOS

- Network Basic Input/Output System
- For network calls to remote devices
  - Session Mode
    - Connection oriented
  - Datagram Mode
    - Connectionless
- Session Layer, Layer 5

Coming Up!

- Next we will continue on with Domain 4 and Network Architecture starting with Multilayer Protocols

*

Multilayer Protocols

- SCADA
- MODBUS
- DNP3

SCADA

- SCADA is a supervisory control and data acquisition system. They are the type of systems that monitor and control industrial processes using computers.
- For example, the monitoring and controlling of processes for power plants, and oil or gas transmission lines would be considered large scale systems and food or auto manufacturing are considered smaller scale systems
- They may also be known as Industrial Control Systems (ICS) or Distributed Control Systems (DCS).

MODBUS

- Simple communication protocol; Similar to Telnet and FTP.
- Considered a client/server type of architecture where the client sends a request to a server and the server responds.
- The client is considered the master and the server is the slave in this architecture
- This protocol was also designed to constantly poll the servers (controllers) for information
- Security such as confidentiality, authentication, authorization, integrity, or access control was not designed within this protocol

DNP3

- Is a more recent communication protocol than Modbus
- Originally designed for electrical systems
- Has some improvements over Modbus include: rather than using polling to determine changes, DNP3 servers (controllers) can initiate responses when a change is detected
- A DNP3 server (controller) can send multiple responses in a single response to multiple requests from a client

Multilayer Protocols

- Still issues with security
- Some of these systems have been ported to more traditional operating systems (windows, Linux)
  - Requires patching

- Some systems may be remote and require remote access where now they are on the Internet

Converged Protocols

- A converged IP network is a single platform on which interoperable devices can be run in innovative ways
- Fewer network components
- Very scalable
- Better utilization of resources using solutions like QoS

Converged Protocols

- FCoE - Fiber Channel over Ethernet
    - Lightweight encapsulation protocol and lacks the reliable data transport of the TCP layer.
    - It does not incorporate TCP or even IP protocols
        - This means that FCoE is a layer 2 (non-routable) protocol just like FC
    - For short-haul communication within a data center
- MPLS - Multi-Protocol Label Switching
    - Best summarized as a layer 2.5 networking protocol. In the traditional OSI model, layer 2 covers protocols like Ethernet and SONET, which can carry IP packets but only over simple LANs or point-to-point WANs. Layer 3 covers Internet-wide addressing and routing using IP protocols
    - MPLS sits between these traditional layers, providing additional features for the transport of data across the network
    - MPLS allows fewer route look ups for routers along the path

Converged Protocols

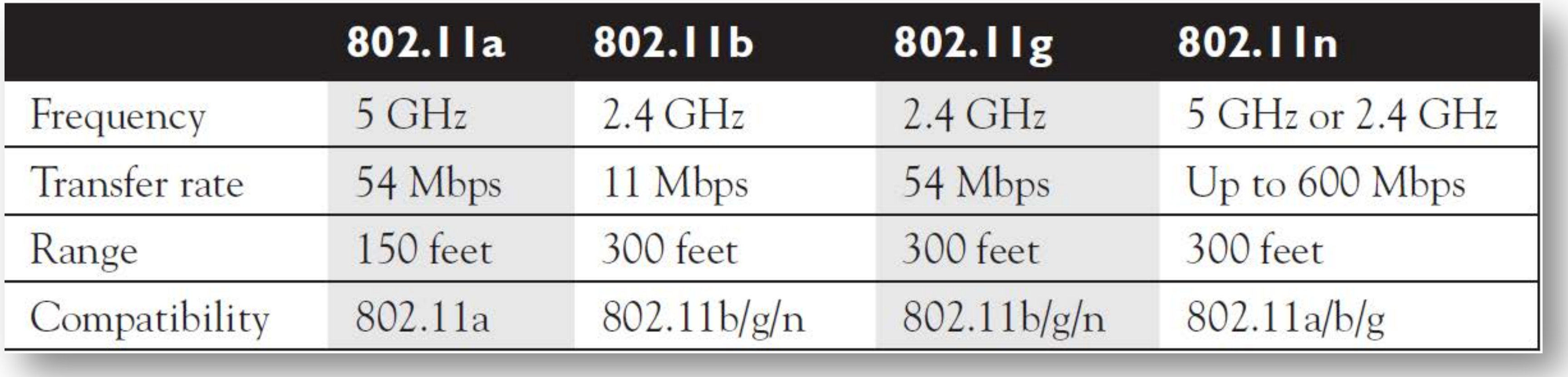
- iSCSI – Internet Small Computer System Interface
  - IP based (Routable)
  - Often seen as a low-cost alternative to Fibre Channel
  - Very popular in datacenters for SANs

- VOIP – Voice over IP
  - Make voice calls using a broadband Internet connection instead of a regular (or analog) phone line

Understanding Wireless Networking

- Modes
  - Infrastructure Mode
  - Ad Hoc Mode

- Standards
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n



	802.11a	802.11b	802.11g	802.11n
Frequency	5 GHz	2.4 GHz	2.4 GHz	5 GHz or 2.4 GHz
Transfer rate	54 Mbps	11 Mbps	54 Mbps	Up to 600 Mbps
Range	150 feet	300 feet	300 feet	300 feet
Compatibility	802.11a	802.11b/g/n	802.11b/g/n	802.11a/b/g

Wireless Networking Security

Three technologies are used to communicate in the 802.11 standard and provide backward compatibility:

- Direct-Sequence Spread Spectrum (DSSS)
- Frequency-Hopping Spread Spectrum (FHSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

Direct-Sequence Spread Spectrum (DSSS)

- Direct-sequence spread spectrum is a wireless technology that spreads a transmission over a much larger frequency band, and with corresponding smaller amplitude. By spreading the signal over a wider band, the signal is less susceptible to interference at a specific frequency.

Frequency-Hopping Spread Spectrum (FHSS)

- This wireless technology spreads its signal over rapidly changing frequencies
- Each available frequency band is subdivided into sub-frequencies
- Signals rapidly hop among these sub-frequencies in an order that is agreed upon between the sender and receiver
- A benefit of FHSS is that the interference at a specific frequency will affect the signal during a short interval

Orthogonal Frequency Division Multiplexing (OFDM)

- A signal is subdivided into sub-frequency bands, and each of these bands is manipulated so that they can be broadcasted together without interfering with each other
- In an OFDM system, each tone is considered to be independent (orthogonal) to the adjacent tones and, therefore, does not require a guard band

Understanding Wireless Networking

- Channels
  - 2.4Ghz
  - 5.0Ghz

- Antenna Types
  - Omnidirectional
  - Directional

Understanding Wireless Networking

- Authentication and Encryption
  - WEP – Wired Equivalent Privacy
    - 64bit and 128bit keys
    - Weak; Cracked!
  - WPA – WiFi Protected Access
    - 128bit key
    - TKIP – Temporal Key Integrity Protocol
    - EAP – Extensible Authentication Protocol
      - For Authentication
      - 2 Flavors
        - LEAP
        - PEAP

Understanding Wireless Networking

- WPA Personal
    - Preshared Keys
- WPA Enterprise
    - Authentication Server
        - RADIUS for example
- WPA2
    - CCMP with AES
        - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
        - Advanced Encryption Standard
        - 128bit, 192bit or 256bit encryption

Securing a Wireless Network

- Best Practices
  - Change Default Configs
    - Admin password or lack of
  - Service Set Identifier (SSID)
  - MAC Address Filtering
  - Antenna Placement and Power Levels
  - Captive Portal (think hotel)
  - Encrypt Wireless Traffic
  - VPN Solutions

Securing a Wireless Network

- Vulnerabilities in Wireless
  - Data Emanation
  - Jamming/Interference
  - Packet Sniffing
  - War Driving and War Chalking
  - SSID Broadcasting
  - WPS and Replay Attacks
  - BlueJacking and Bluesnarfing
  - Rouge Access Points/Evil Twins
  - Weak Encryption/IV Attacks

Cryptography used to maintain communications security

- Public Key Cryptography
  - PKI
  - Asynchronous
- Symmetric-Key Encryption
  - Pre Shared Key
- Digital Signatures

Cryptography used to maintain communications security

- Certificates
  - **Client SSL certificates** – Used to identify clients to servers via SSL (client authentication)
  - **Server SSL certificates** – Used to identify servers to clients via SSL (server authentication)
  - **S/MIME certificates** – Used for signed and encrypted email.
  - **Object-Signing certificates** – Used to identify signers of program code, scripts, or other signed files
  - **Certificate Authority (CA) certificates** – Used to identify CAs

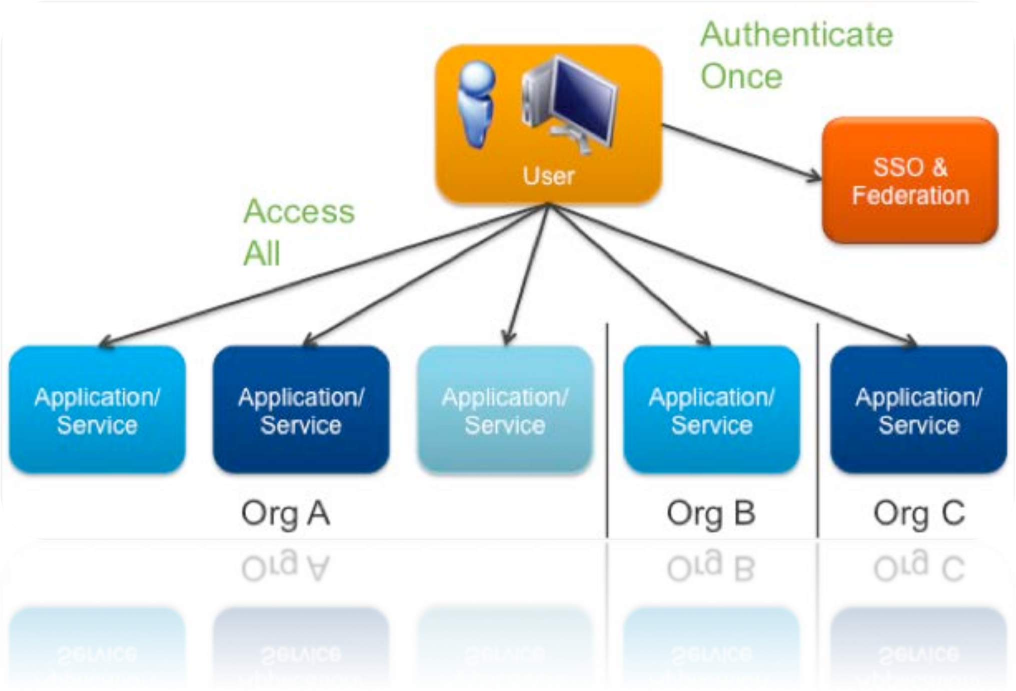
Single Sign-On

- A users identity is shared across multiple applications
- Authenticate one time and that authentication follows throughout the session – app to app
- Lots of pros but lots of cons as well
  - Pros
    - Easier to Admin
    - Easier for users (one password, one login)
    - Timeouts and thresholds across all apps
  - Cons
    - Harder to implement correctly
    - Expensive
    - Could have single point of failure

SSO Risks

- Single point of failure
  - All credentials in one location

- Single Point of Access
  - DDoS on that server will cause authentication issues



Coming Up!

- Next we will continue on with Domain 4 and start talking about Secure Network Components

*

Securing network components

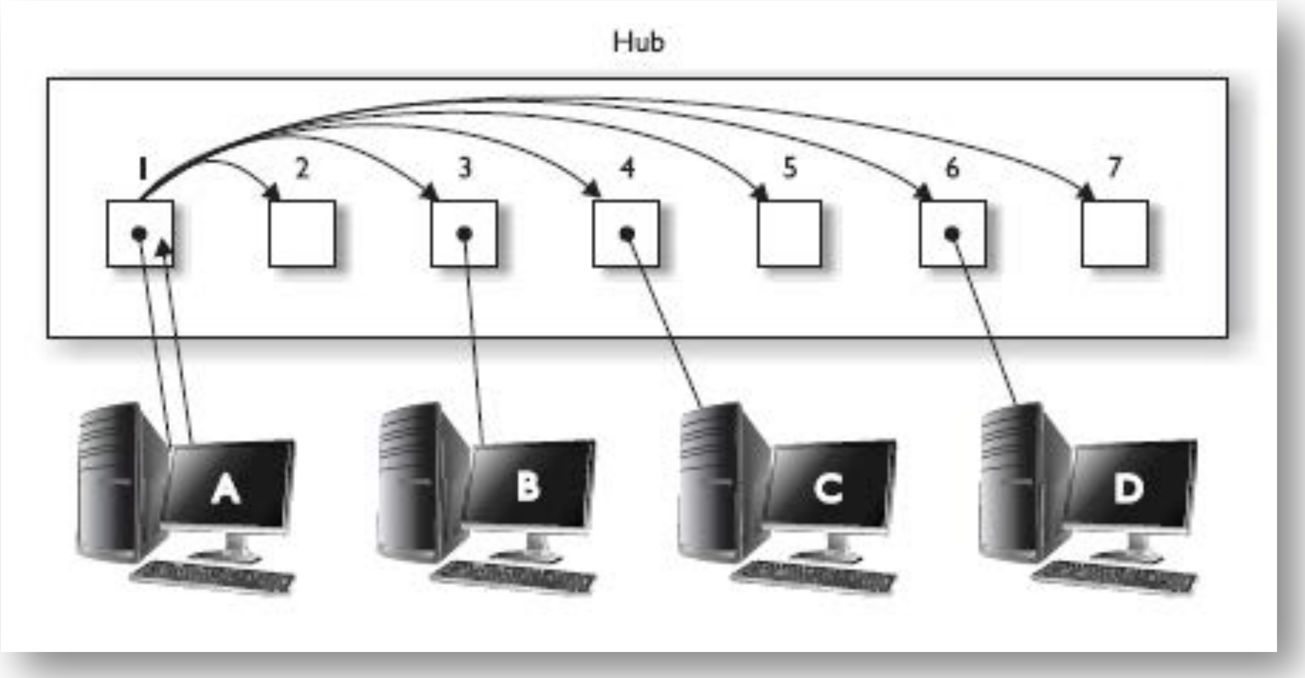
- Operation of hardware
- Transmission media
- Network access control devices
- Endpoint security
- Content distribution networks

Operation of hardware

- Hub
- Switch
- Router
- Load Balancer

Hub

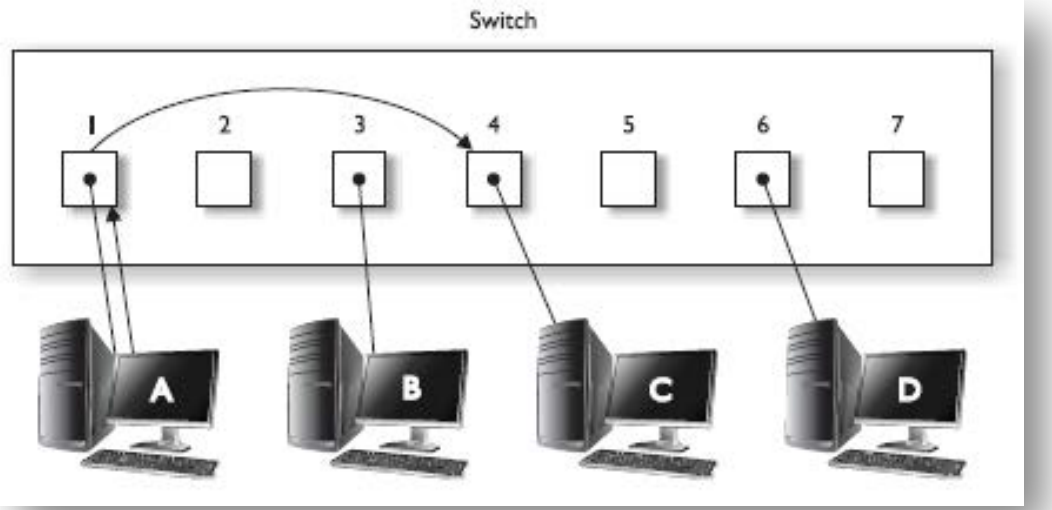
- Layer 1 Device
- Repeats signal out all active ports
  - Think of a power strip



Switch

- Layer 2 or 3 device
  - MAC address or IP Address

- Has a MAC Address Table
  - Allows traffic to go to just the destined device
    - Can run at full duplex
      - Send and Receive at the same time

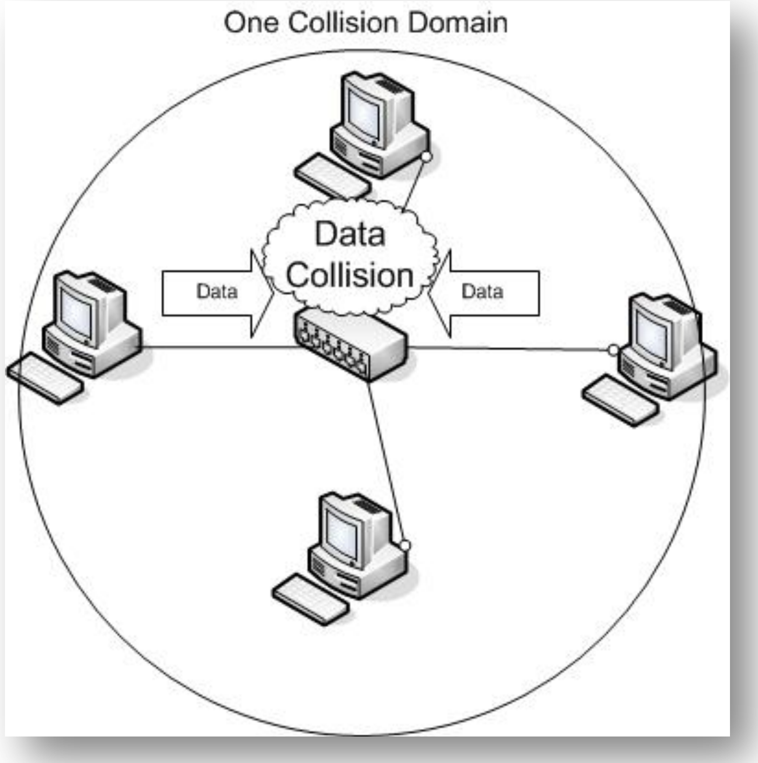


Switch

- Other benefits
    - Filtering
        - Filter out traffic
    - Port Mirroring
        - What comes/goes on one port is identical to another
    - Port Security
        - Decides what devices can use a port on a specific switch
    - Disable Ports
        - If someone plugs into a port that doesn’t “belong” can do “something”

Collision Domains

- Group of devices on the same segment
- Only one device on the segment can talk at once



VLANs

- Virtual Local Area Networks

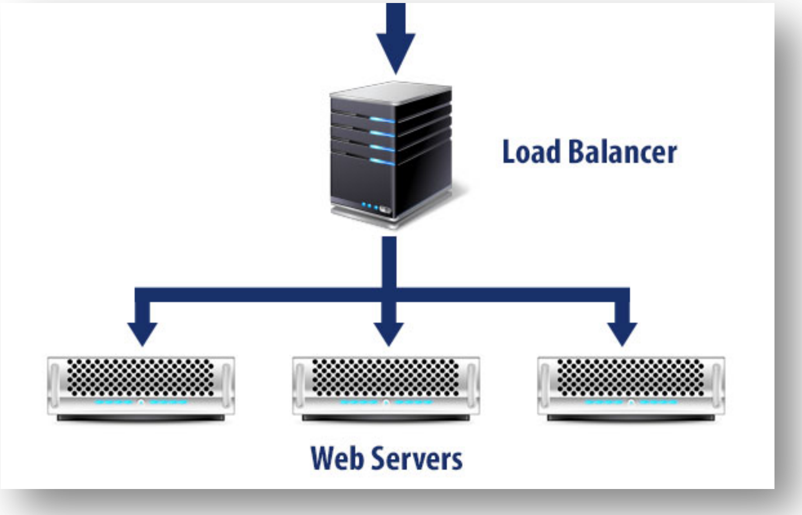
- Using the same hardware but virtually/logically separating the traffic

Router

- Layer 3 device
- Separates or brings together different networks
- Routes traffic based on destination IP address
- Separate our broadcast domains

Load Balancer

- Splits the load between devices like servers and routers
- Supposed to improve performance for services



Transmission Media

Let’s take a look at the three types of popular cables used:

- Coaxial
- Twisted pair
- Fiber optic

Coax

- *Coaxial* cable, referred to as *coax*, contains a center conductor made of copper that's surrounded by a plastic jacket with a braided shield over it.
- A plastic such as polyvinyl chloride (PVC, commonly known as Teflon) covers this metal shield.
- The Teflon-type covering is frequently referred to as a *plenum-rated coating*, and it's often mandated by local or municipal fire code when cable is hidden in walls and ceilings.

Twisted-Pair Cable

- Twisted-pair cable consists of multiple individually insulated wires that are twisted together in pairs
- Sometimes a metallic shield is placed around them; *shielded twisted-pair (STP)*
- Cable without outer shielding is called *unshielded twisted-pair (UTP)*, and it's used in twisted-pair Ethernet (10Base-T, 100Base-TX, 1000Base-TX) networks
- So why are the wires in this cable type twisted? Because when electromagnetic signals are conducted on copper wires in close proximity—like inside a cable—it causes interference called *crosstalk*. Twisting two wires together as a pair minimizes interference and even protects against interference from outside sources.

Unshielded Twisted-pair

This cable type is the most common today for the following reasons:

- It’s cheaper than other types of cabling
- It’s easy to work with
- UTP cable is rated in these categories:
  - Cat1
  - Cat2
  - Cat3
  - Cat4
  - Cat5
  - Cat5e
  - Cat6

Fiber Optic

- Because fiber-optic cable transmits digital signals using light impulses rather than electricity, it’s immune to EMI and RFI
- The cable itself comes in either single-mode fiber (SMF) or multimode fiber (MMF); the difference between them is in the number of light rays (the number of signals) they can carry
    - Multimode fiber is most often used for shorter-distance applications and single-mode fiber for spanning longer distances.

Fiber Optic

Pros:

- Is completely immune to EMI and RFI
- Can transmit up to 40 kilometers (about 25 miles)

Cons:

- Is difficult to install
- Is more expensive than twisted-pair
- Troubleshooting equipment is more expensive than twisted-pair test equipment
- Is harder to troubleshoot

Network Access Control

- Firewalls
- Proxy

Understanding Firewalls

- Quite simply – they block/allow traffic in or out of your network

- Types of Firewalls
  - Packet-Filtering
    - Based in IP and port
  - Stateful Packet Inspection
    - Rules and Context
  - Application Layer
    - Other two, plus based on payload of data

Understanding Firewalls

- Topologies
  - Dual-homed Firewalls
  - Screened Firewalls
  - Screened Subnet Firewalls

- Security Zones
  - Private LAN
  - DMZ
  - Public Zone

Proxy

- Proxy Server
  - Works on your behalf
  - Hides internal network

Other Technologies

- Web Application Firewall – WAF
  - Controls the HTTP messages
- Web Security Gateway
  - Can protect from inappropriate content
  - Can provide Data Lose Prevention
  - Can scan for malicious code
- VPN Concentrator
  - Centralize the VPN access
  - Can have authentication and encryption

Other Technologies

- URL Filter
  - List of sites to allow or deny

- Content Inspection
  - Looks at the page content

- Malware Inspection
  - Looking for Malware in your connection

End Point Security

- Up-to-date anti-virus and anti-malware software
- A configured and operational host-based firewall
- A hardened configuration with unneeded services disabled
- A patched and maintained operating system

- What about Mobile systems?
  - Remote wipe
  - Tracking
  - Encryption

Content-Distribution Networks (CDNs)

- A large distributed system of servers deployed in multiple data centers around the Internet
- Key enabling technology behind successful consumer-facing sites in verticals such as media and entertainment, software download delivery, gaming, and ecommerce
- Give content owners and publishers the ability to rapidly scale to meet increasing user demand all over the world on multiple devices and on different platforms
- The goal of a CDN is to serve content to end-users with high availability and high performance

Coming Up!

- Next we will continue on with domain 4 starting with Design and Establish Secure Communication Channels

Design and Establish Secure Communication Channels

- Voice
- Multimedia Collaboration
- Remote Access
- Data Communications
- Virtualized Networks

Voice

- PSTN – Public Switched Telephone Network
    - circuit-switched network that was originally designed for analog voice communication
    - Susceptible to War Dialing and Phone Hacking (Phreaking)
- POTS – Plain Old Telephone System
- PBX – Private Branch Exchange
    - Internal switch to route calls coming in
    - Susceptible to War Dialing

Multimedia Collaboration

- Peer-to-Peer Applications (P2P)
  - Throttling applied
  - Ports blocked or monitored
- Remote Meeting Technology
- Instant Messaging
  - Web Based
  - Enterprise level
  - Jabber
  - Internet Relay Chat (IRC)

Remote Access

- Virtual Private Network (VPN)
- Point-to-Point Tunneling Protocol (PPTP)
    - Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol that runs over other protocols. PPTP relies on generic routing encapsulation (GRE) to build the tunnel between the end points
- Layer 2 Tunneling Protocol (L2TP)
    - It allows callers over a serial line using PPP to connect over the Internet to a remote network

Remote Access

- Remote Authentication Dial-in User Service (RADIUS)
  - RADIUS is an authentication protocol used mainly in networked environments

- Telnet
- Screen Scraper
  - program that can extract data from output on a display intended for a human

- Virtual Applications and Desktops
- Telecommuting

IP Security (IPSec)

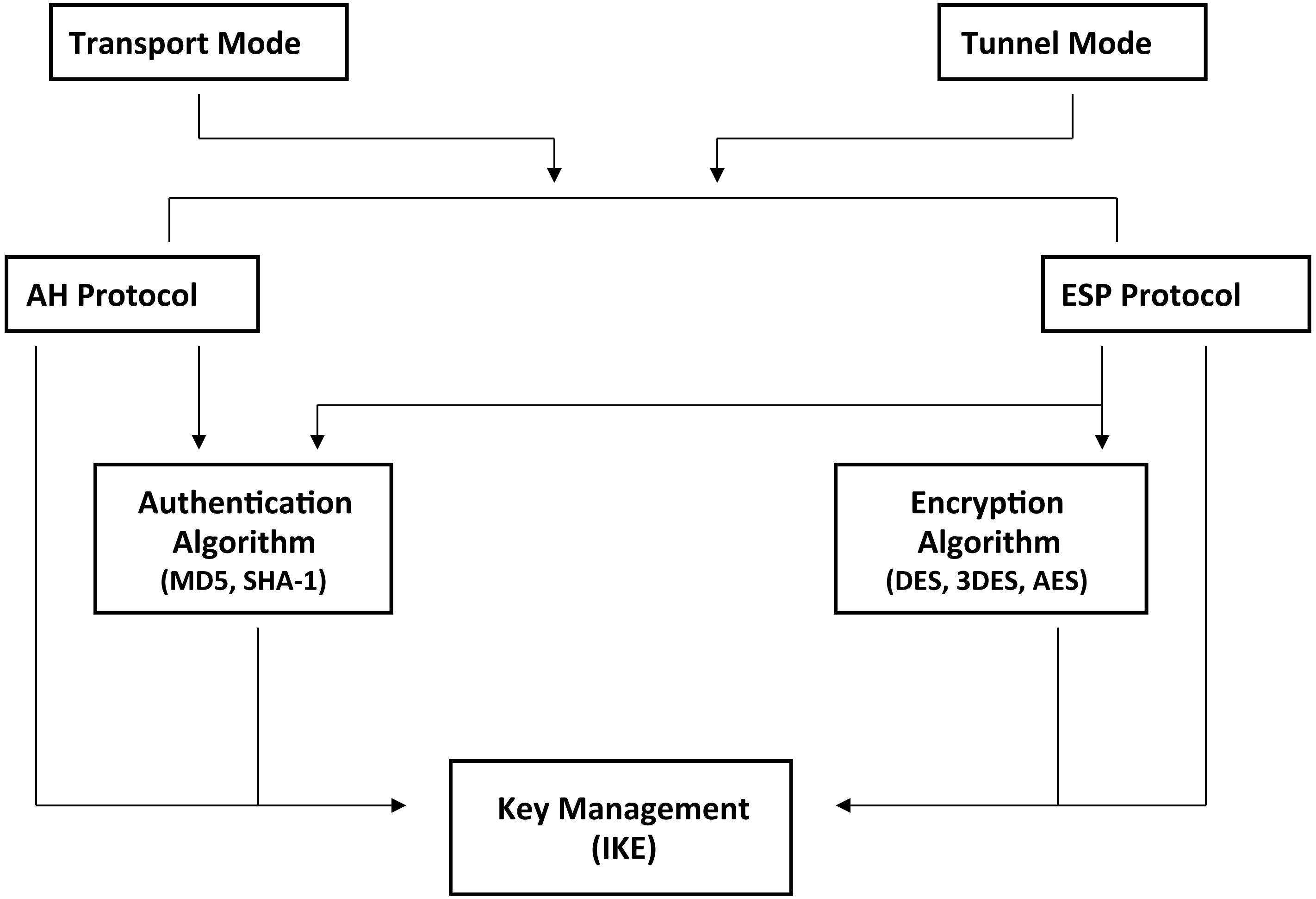
- **Security Architecture for IP**

  - open standard defined in RFC 2401
  - consists of a suite of security services & protocols
  - operates at layer 3 of OSI model
  - provides security for layer 3 and above (4 – 7)

- **Three Major Components of IPSec**

  - Modes: Transport & Tunnel
  - Protocols: AH & ESP
  - Internet Key Exchange (IKE)

IPSec Architecture



Transport Mode

Tunnel Mode

AH Protocol

ESP Protocol

Authentication Algorithm (MD5, SHA-1)

Encryption Algorithm (DES, 3DES, AES)

Key Management (IKE)

AH & ESP

- Authentication Header (AH)
  - IP Protocol 51, RFC 2402
  - provides authentication and anti-replay services
  - does not encrypt IP packet payload

- Encapsulating Security Payload (ESP)
  - IP Protocol 50, RFC 2406
  - provides authentication, optional anti-replay services, & packet payload encryption
  - can be used as stand alone or in conjunction with AH

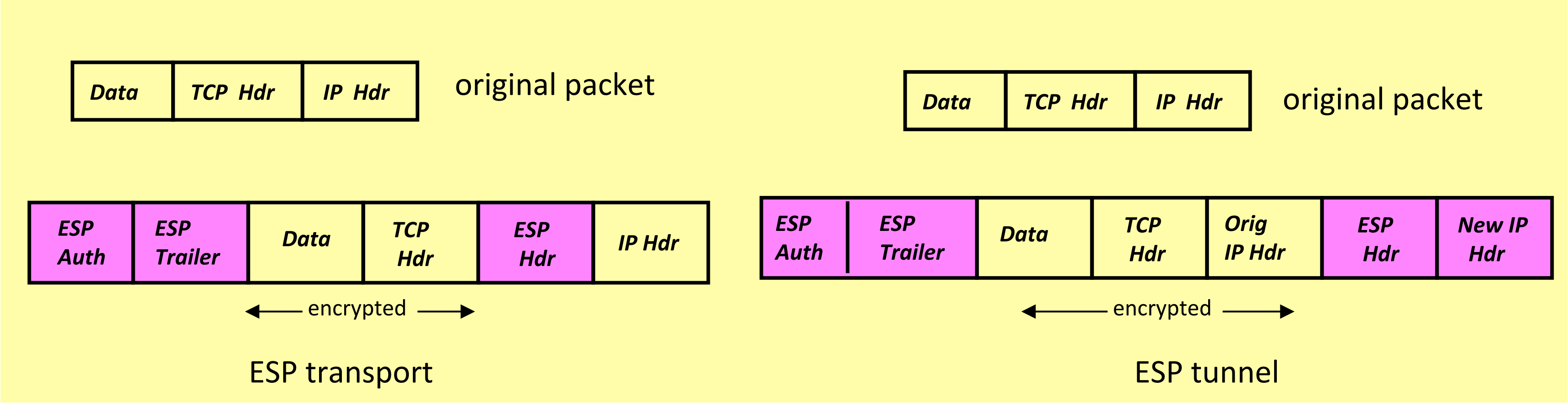
AH & ESP Modes

- **Transport**

  - authenticates/encrypts only data payload
  - original IP header remains intact

- **Tunnel**

  - authenticates/encrypts entire IP packet
  - adds new IP header



Authentication & Encryption Algorithms

- HMAC-MD5
- HMAC-SHA-1

authentication

- DH - key exchange

- DES
- 3DES
- AES

payload encryption

Data Communications

- Analog vs. Digital
- Secure Shell (SSH)
    - Services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel
- SSL/ TLS
    - VPNs SSL 3.0 (Secure Socket Layer) and TLS 1.2 (Transport Layer Security) are compatible, with SSL being a session encryption tool that was developed by Netscape and TLS 1.2 being the open standard IETF version of SSL 3

Virtualized Networks

- Virtualization
  - Adds a software layer between an operating system and the underlying computer hardware. This allows multiple guest operating systems to run simultaneously on one physical host computer.

Virtualized Networks

- Hypervisor
  - The key to virtualization security is the hypervisor, which controls access between virtual guests and host hardware. A type 1 hypervisor (also called bare metal) is part of an operating system that runs directly on host hardware. A type 2 hypervisor runs as an application on a normal operating system, such as Windows 7.
  - Many virtualization exploits target the hypervisor, including hypervisor-controlled resources shared between host and guests, or guest and guest. These include cut-and-paste, shared drives, and shared network connections.

Virtualized Networks

- Software Designed Network
  - The purpose of SDN is to separate traditional network traffic into three components: raw data, how the data is sent, and what purpose the data serves
- **Infrastructure Layer or Data Plane** – Network switches and routers and the data itself as well as the process of forwarding data to the appropriate destination.
- **Control Layer or Control Plane** – The intelligence in devices that works in true middle-man fashion, determining how traffic should flow based on the status of the infrastructure layer and the requirements specified by the application layer.
- **Application Layer or Application Plane** – Network services, utilities, and applications that interface with the control level to specify needs and requirements

Virtualized Networks

- Virtual SAN
  - Software-defined storage (SDS) offering from VMware that enables enterprises to pool their storage capabilities
  - To instantly and automatically provision virtual machine storage via simple policies that are driven by the virtual machine

Mitigate Network Attacks

- Bluejacking and bluesnarfing
  - With Bluetooth technology becoming wildly popular, several new attack methods have evolved, including bluejacking (sending anonymous, unsolicited messages to Bluetooth-enabled devices) and bluesnarfing (stealing personal data, such as contacts, pictures, and calendar information from a Bluetooth-enabled phone). Even worse, in a bluesnarfing attack, information about your cellular phone (such as its serial number) can be downloaded, then used to clone your phone.
- Fraggle
  - This attack is a variant of a Smurf that uses UDP Echo packets (UDP port 7) rather than ICMP packets. Cisco routers can be configured to disable the TCP and UDP services (known as TCP and UDP small servers) that are most commonly used in Fraggle attacks.

Mitigate Network Attacks

- Session hijacking (spoofing)
  - IP spoofing involves altering a TCP packet so that it appears to be coming from a known, trusted source, thus giving the attacker access to the network.
- SYN flood
  - In a SYN flood attack, TCP packets with a spoofed source address request a connection (SYN bit set) to the target network. The target responds with a SYN-ACK packet, but the spoofed source never replies. Half-open connections are incomplete communication sessions awaiting completion of the TCP three-way handshake. These connections can quickly overwhelm a system's resources while the system waits for the half-open connections to time out, which causes the system to crash or otherwise become unusable.

SYN flood Mitigation

- SYN floods are countered on Cisco routers by using two features: TCP Intercept, which effectively proxies for the half-open connections and Committed Access Rate which limits the bandwidth available to certain types of traffic
- Checkpoint's firewall has a feature known as SYN Defender that functions in way similar to the Cisco TCP Intercept feature
- Other defenses include changing the default maximum number of TCP half-open connections and reducing the timeout period on networked systems.

Mitigate Network Attacks

- Teardrop
  - In a Teardrop attack, the Length and Fragmentation offset fields of sequential IP packets are modified, causing the target system to become confused and crash.
- UDP flood
  - In a UDP flood attack, large numbers of UDP packets are sent to the target network to consume available bandwidth and/or system resources. UDP floods can generally be countered by dropping unnecessary UDP packets at the router. However, if the attack uses a required UDP port (such as DNS port 53), other countermeasures need to be employed.

Mitigate Network Attacks

- ICMP flood
  - In an ICMP flood attack, large numbers of ICMP packets (usually Echo Request) are sent to the target network to consume available bandwidth and/or system resources. Because ICMP isn't required for normal network operations, the easiest defense is to drop ICMP packets at the router or filter them at the firewall
- Smurf
  - A Smurf attack is a variation of the ICMP flood attack. In a Smurf attack, ICMP Echo Request packets are sent to the broadcast address of a target network by using a spoofed IP address on the target network. The target then transmits the ICMP Echo Request to all hosts on the network. Each host then responds with an Echo Reply packet, overwhelming the available bandwidth and/or system resources. Countermeasures against Smurf attacks include dropping ICMP packets at the router.

Domain 4 Complete!

- Apply Secure Design Principles to network Architecture
- Securing network components
- Secure communication channels
- Prevent or mitigate network attacks

CISSP

Domain 5

Identity and Access Management

(Controlling Access and Managing Identity)

Key Areas

- Controlling Access to Assets
- Identification and Authentication
- Identity as a Service
- Third-Party Identity Services
- Authorization Mechanisms
- Access Control Attacks
- Manage the Identity and Access Provisioning Lifecycle

Confidentiality, integrity, and availability

- Confidentiality
  - Seeks to prevent the unauthorized disclosure of information: it keeps data secret. In other words, confidentiality seeks to prevent unauthorized read access to data. An example of a confidentiality attack would be the theft of Personally Identifiable Information (PII), such as credit card information.
- Integrity
  - Seeks to prevent unauthorized modification of information. In other words, integrity seeks to prevent unauthorized write access to data
- Availability
  - Ensures that information is available when needed. Systems need to be usable (available) for normal business use. An example of attack on availability would be a Denial-of-Service (DoS) attack, which seeks to deny service (or availability) of a system

DAD

- Disclosure, Alteration, and Destruction
  - The CIA triad may also be described by its opposite: Disclosure, Alteration, and Destruction (DAD)
- Disclosure is the unauthorized disclosure of information
- Alteration is the unauthorized modification of data
- Destruction is making systems unavailable

Identity and Authentication, Authorization, and Accountability

- The term “AAA” is often used, describing cornerstone concepts Authentication, Authorization, and Accountability
- Left out of the AAA acronym is Identification, which is required before the three “A's” can follow

Identity and Authentication, Authorization, and Accountability

- Identity and authentication Identity is a claim: if your name is “Mark,” you identify yourself by saying “I am Mark” but Identity alone is weak because there is no proof.
- Proving an identity claim is called **authentication**: you authenticate the identity claim, usually by supplying a piece of information or an object that only you posses, such as a password or your passport

Identity and Authentication, Authorization, and Accountability

- Authorization
  - Describes the actions you can perform on a system once you have identified and authenticated. Actions may include reading, writing, or executing files or programs.
- Accountability
  - Holds users accountable for their actions. This is typically accomplished by logging and analyzing audit data. Enforcing accountability helps keep the honest people honest.

Terminology

- Nonrepudiation
  - Means a user cannot deny (repudiate) having performed a transaction. It combines authentication and integrity: nonrepudiation authenticates the identity of a user who performs a transaction and ensures the integrity of that transaction
- Least privilege and need to know
  - Least privilege means users should be granted the minimum amount of access (authorization) required to do their jobs, but no more. Least privilege is applied to groups of objects
  - Need to know is more granular than least privilege: the user must need to know that specific piece of information before accessing it

Terminology

- Subjects and Objects
  - Subject is an active entity on a data system. Most examples of subjects involve people accessing data files. However, running computer programs are subjects as well. An object is any passive data within the system
  - Objects can range from databases to text files. The important thing to remember about objects is that they are passive within the system. They do not manipulate other objects
- Defense-in-depth
  - Applies multiple safeguards or controls to protect an asset. Any single security control may fail but by deploying multiple controls, you improve the confidentiality, integrity, and availability of your data.

Controlling Access to Assets

- Preventive controls, for reducing risk
- Detective controls, for identifying violations and incidents
- Corrective controls, for remedying violations and incidents and improving existing preventive and detective controls
- Deterrent controls, for discouraging violations
- Recovery controls, for restoring systems and information
- Compensating controls, for providing alternative ways of achieving a task

Controlling Access to Assets

- Preventive technical controls include
  - Encryption: Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
  - Access control mechanisms: Biometrics, smart cards, and tokens
  - Access control lists: Permission lists that define what a subject can or cannot do to an object
  - Remote access authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP)
- Detective technical controls include
  - Violation reports
  - Audit trails
  - Network monitoring and intrusion detection
- Although technical controls are primarily preventive and detective, you may also use them for corrective, deterrent, and recovery purposes.

Controlling Access to Assets

- Physical controls ensure the safety and security of the physical environment. These are primarily preventive or detective in nature.
- Preventive physical controls include
  - Security perimeters, such as fences, locked doors, and restricted areas
  - Guards and dogs
- Detective physical controls include
  - Motion detectors
  - Video cameras
- Often, physical controls are also deterrent in nature. For example, fences, locked doors, security guards and dogs, motion detectors, and video cameras, in addition to being preventive and detective controls, also function as effective deterrent controls, in many cases.

Identification and Authentication

- Single sign-on Single Sign-On (SSO) allows multiple systems to use a central authentication server (AS).
- This allows users to authenticate once and then access multiple, different systems.
- It also allows security administrators to add, change, or revoke user privileges on one central system.
- The primary disadvantage to SSO is it may allow an attacker to gain access to multiple resources after compromising one authentication method, such as a password
    - SSO should always be used with multifactor authentication for this reason

Identification and Authentication

- Federated Identity Management applies Single Sign-On at a much wider scale: ranging from cross organization to Internet scale.
- It is sometimes simply called Identity Management.
- Federated Identity Management may use OpenID or SAML (Security Association Markup Language)
- With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled
- Federated identity management permits extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations

Kerberos

- Kerberos is a third-party authentication service that may be used to support Single Sign-On.
- Kerberos uses symmetric encryption and provides mutual authentication of both clients and servers. It protects against network sniffing and replay attacks.

Kerberos Components

- Principal: Client (user) or service
- Realm: A logical Kerberos network
- Ticket: Data that authenticates a principal's identity
- Credentials: A ticket and a service key
- KDC: Key Distribution Center, which authenticates principals
- TGS: Ticket-Granting Service
- TGT: Ticket-Granting Ticket
- C/ S: Client/ Server, regarding communications between the two

SESAME

- SESAME is Secure European System for Applications in a multivendor environment, a single sign-on system that supports heterogeneous environments.
- SESAME can be thought of as a sequel of sorts to Kerberos

Coming Up!

- Next we will continue with Domain 5 starting with Identification and Authentication

*

Identification and Authentication

- A key concept for implementing any type of access control is controlling the proper authentication of subjects within the IT system.
- A subject first identifies himself or herself; this identification cannot be trusted. The subject then authenticates by providing an assurance that the claimed identity is valid. A credential set is the term used for the combination of both the identification and authentication of a user
- There are three basic authentication methods:
  - Type 1 (something you know)
  - Type 2 (something you have)
  - Type 3 (something you are)

Something You Know

- Type 1 authentication (something you know) requires testing the subject with some sort of challenge and response where the subject must respond with a knowledgeable answer

- Look out for:
  - Password hashes and password cracking
  - Dictionary attacks
  - Hybrid attacks
  - Brute Force Attacks
  - Rainbow tables

Something You Have

- Type 2 authentication (something you have) requires that users possess something, such as a token, which proves they are an authenticated user.
- A token is an object that helps prove an identity claim
- Smart Cards

Something You Are

- Type 3 authentication (something you are) is biometrics, which uses physical characteristics as a means of identification or authentication.
- Biometrics may be used to establish an identity or to authenticate

- The accuracy of biometric systems should be considered before implementing a biometric control program.
- Three metrics are used to judge biometric accuracy:
  - The False Reject Rate (FRR)
  - The False Accept Rate (FAR)
  - The Crossover Error Rate (CER).

False reject rate

- A false rejection occurs when an authorized subject is rejected by the biometric system as unauthorized.
- False rejections are also called a Type I error.
- False rejections cause frustration of the authorized users, reduction in work due to poor access conditions, and expenditure of resources to revalidate authorized users.

False accept rate

- A false acceptance occurs when an unauthorized subject is accepted as valid. If an organization's biometric control is producing a lot of false rejections, the overall control might have to lower the accuracy of the system by lessening the amount of data it collects when authenticating subjects.
- When the data points are lowered, the organization risks an increase in the false acceptance rate.
  - The organization risks an unauthorized user gaining access.
- This type of error is also called a Type II error

Crossover Error Rate

- The Crossover Error Rate (CER) describes the point where the False Reject Rate (FRR) and False Accept Rate (FAR) are equal.
- CER is also known as the Equal Error Rate (EER). The Crossover Error Rate describes the overall accuracy of a biometric system.
- As the sensitivity of a biometric system increases, FRRs will rise and FARs will drop.
- Conversely, as the sensitivity is lowered, FRRs will drop and FARs will rise

Types of biometric controls

- Iris Scan
- Retina Scan
- Finger Printing
- Voice Recognition
- Facial Scan
- Keyboard Dynamics
- Hand Geometry

Session Management

- Session management is a term used to describe how a single instance of identification and authentication is applied to resources
- Web browsers rely on sessions to manage access to Web applications and resources often through the use of cookies or other session monitoring and tracking technologies
  - While session management provides ease of use and flexibility for the end-user, it also provides an avenue of attack.

Session Management

- Desktop sessions can be controlled and protected through different means as well
  - Screensavers
  - Timeouts
  - Automatic Logouts
  - Session/Login limitation
  - Schedule Limitation

Identity as a Service (IDaaS)

- Identity-as-Service (IDaaS) offerings are cloud-based services that broker identity and access management functions to target systems on customers' premises and in the cloud
- Combination of administration and account provisioning, authentication and authorization, and reporting functions

Authorization Mechanisms

- Access control models
  - MAC
    - Mandatory Access Control
  - DAC
    - Discretionary Access Control
  - RBAC
    - Role Based Access Control
  - Rule Based Access Control

Mandatory Access Controls

- Mandatory Access Control (MAC) is system-enforced access control based on subject's clearance and object's labels.
- Subjects and objects have clearances and labels, respectively, such as confidential, secret, and top secret
- A subject may access an object only if the subject's clearance is equal to or greater than the object's label.
- Subjects cannot share objects with other subjects who lack the proper clearance or “write down” objects to a lower classification level (such as from top secret to secret)
- MAC systems are usually focused on preserving the confidentiality of data.

Discretionary Access Controls

- Discretionary Access Control (DAC) gives subjects full control of objects they have been given access to, including sharing the objects with other subjects
- Subjects are empowered and control their data. Standard UNIX and Windows operating systems use DAC for file systems: subjects can grant other subjects access to their files, change their attributes, alter them, or delete them

Role-Based Access Control

- Role-Based Access Control (RBAC) defines how information is accessed on a system based on the role of the subject. A role could be a nurse, a backup administrator, a help desk technician, etc.
- Subjects are grouped into roles and each defined role has access permissions based upon the role, not the individual.
- Type of nondiscretionary access control because users do not have discretion regarding the groups of objects they are allowed to access and are unable to transfer objects to other subjects

Nondiscretionary access control

- Task-based access control is another nondiscretionary access control model, related to RBAC.
- Task-based access control is based on the tasks each subject must perform, such as writing prescriptions, restoring data from a backup tape, or opening a help desk ticket
- It attempts to solve the same problem that RBAC solves, focusing on specific tasks, instead of roles

Rule-based access

- A rule-based access control system uses a series of defined rules, restrictions, and filters for accessing objects within a system.
- The rules are in the form of "if/then" statements.
- An example of a rule-based access control device is a proxy firewall that allows users to surf the Web with predefined approved content only (If the user is authorized to surf the Web and the site is on the approved list, then allow access). Other sites are prohibited and this rule is enforced across all authenticated users

Access Control Attacks

- **Brute-force or dictionary attack**: The attacker attempts every possible combination of letters, numbers, and characters to crack a password, passphrase, or PIN. A dictionary attack is essentially a more focused type of brute force attack in which the attacker uses a predefined word list.
    - You can find such word lists or dictionaries, including foreign language and special-interest dictionaries, widely available on the Internet for use in password-cracking utilities such as L0phtCrack and John the Ripper.
    - Attackers typically run these password-cracking utilities against a copy of the target system's (or network's) security accounts database or password file. The utility creates hashes of passwords contained in its dictionary or word list, and then compares the resulting hash to the password file.
    - These types of programs work very quickly and effectively even when organizations use complex passwords, so the key to defending against a brute-force or dictionary attack is to protect your security accounts databases and password files.

Access Control Attacks

- **Man-in-the-Middle attacks**: Here an attacker intercepts messages between two parties and forwards a modified version of the original message to the intended recipient. For example, an attacker may substitute his or her own public key during a public-key exchange between two parties. The two parties believe that they're still communicating only with each other and unknowingly encrypt messages by using the attacker's public key, rather than the intended recipient's public key. The attacker can then decrypt secret messages between the two parties, modify their contents as desired, and send them on to the unwary recipient.
- **Packet sniffing**: An attacker uses an application or device, known as a sniffer, to capture network packets and analyze their contents, such as usernames and passwords, and shared keys.

Access Control Attacks

- **Buffer or stack overflows** constitute the most common and successful type of computer attacks today. Although often used in Denial of Service attacks, buffer overflows in certain systems or applications may enable an attacker to gain unauthorized access to a system or directory.
- An overflow occurs when an application or protocol attempts to store more information than the allotted resources will allow. This causes previously entered data to become corrupted, the protocol or application to crash, or other unexpected or erratic behavior to occur.
  - A teardrop attack is a type of stack overflow attack that exploits vulnerabilities in the IP protocol. The best defense against buffer or stack overflow attacks is to identify and patch vulnerabilities in the system, network, and applications as quickly as possible after each vulnerability is identified (and ideally before the affected code or application is used in a production environment).

Access Control Attacks

- **Session hijacking**: Similar to a Man-in-the-Middle attack, except that the attacker impersonates the intended recipient, instead of modifying messages in transit.
- **Social engineering**: This low-tech method is one of the most effective and easily perpetrated forms of attack. Common techniques involve phishing, dumpster diving, shoulder surfing, raiding cubicles (looking for passwords on monitors, under keyboards, and under mouse pads), and plain asking.
    - This latter brazen technique can simply involve the attacker calling a user, pretending to be a system administrator and asking for the user's password, or calling a help desk pretending to be a user and asking to have the password changed

Access provisioning lifecycle

- Once the proper access control model has been chosen and deployed, the access provisioning lifecycle must be maintained and secured.
- Many organizations follow best practices for issuing access but lack formal processes for ensuring the entire lifetime of access is kept secure as employees and contractors move within an organization

Domain 5 Complete!

- Controlling Access to Assets
- Identification and Authentication
- Identity as a Service
- Third-Party Identity Services
- Authorization Mechanisms
- Access Control Attacks
- Manage the Identity and Access Provisioning Lifecycle

CISSP

Domain 6

Security Assessment and Testing

(Designing, Performing and Analyzing Security Testing)

Key Areas

- Assessment and Test Strategies
- Security Control Testing
- Collect Security Process Data
- Analyze and Report Test Outputs
- Conduct or Facilitate Internal and Third-Party Audits

Assessment and Test Strategies

- Look at the industry standards
- Follow Regulations and Laws
- Evaluate test plans and procedures that are applied during development and operational testing
- Work with Vendors and resellers
- Work in a team to design and develop your strategies

Security Control Testing

- Vulnerability Assessment
  - Nessus; GFI Languard; OpenVAS; Retina; SAINT
- Penetration Testing
  - Backtrack; now Kali Linux
- Log Reviews
  - Log is a record of the events occurring within an organization's systems and networks.
  - Logs make up Log Entries
  - Who has access? Where are they stored? How often are they reviewed? What type of information is logged? What can we use this for?
- Synthetic Transactions
  - Putting in fake data to test our systems using scripts to emulate real users

Security Control Testing

- Code Review and Testing
  - Black-Box and White-Box Testing
  - Manual and Automatic Testing
- Misuse Case Testing
  - Are you trapping for errors? Handling mistake properly?
- Interface Testing
  - Conducted to evaluate whether systems or components pass data and control correctly to one another.

Collect Security Process Data

- Account Management
    - Have eyes on our accounts – escalations or revocations
- Management Review
    - Have management involved in the process. Let them review the procedures, requests and approve or deny requests
- Key Performance and Risk Indicators
    - Performance indicators tell us how well we are doing. Are we meeting our goals. Think about Metrics and how can we measure the success (or failure) of our project

Collect Security Process Data

- Backup Verification Data
  - Test your back ups. Don't take for granite that because the backup process ran successfully, the data was backed up properly. Do a test restore to make sure the procedures are still valid along with the data that was restored
- Training and Awareness
  - Get people trained up!
  - Have well written, understandable, policies in place that outline procedures for organizational staff

Analyze and Report Test Outputs

- Once assessments are completed – Analyze the outputs to make sure the metrics are where we need them.
- Are we meeting our stated goals for security posture?

- Report the outputs to everyone requiring access.
    - Team Leads
    - Executive teams
    - Upper Management
    - The Public

Conduct Internal or Facilitate Third-Party Audits

- Conduct internal audits regularly
  - Want to make sure you are keeping in line with stated security goals
    - Policies, Procedures, Access Control, etc...

- Have third-party audits as well to get another perspective or because you are required by law to do so.
  - Ensure proper scoping and tailoring get the appropriate number of controls at the correct level for the target system

Conduct Internal or Facilitate Third-Party Audits

- Establish a security baseline through annual audits
- Spell out your objectives
- Choose auditors with real security experience
- Involve business unit managers early
- Make sure auditors rely on experience, not just checklists
- Insist that the auditor's report reflects your organization's risks

Domain 6 Complete

- Assessment and Test Strategies
- Security Control Testing
- Collect Security Process Data
- Analyze and Report Test Outputs
- Conduct or Facilitate Internal and Third-Party Audits

*

CISSP

Domain 7

Security Operations

(Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

Key Areas

- Investigations
- Requirements for Investigation Types
- Logging and Monitoring Activities
- Provisioning of Resources
- Foundational Security Operations Concepts
- Resource Protection Techniques
- Incident Management
- Preventative Measures

Key Areas

- Path and Vulnerability Management
- Change Management
- Recovery Strategies
- Disaster Recovery Process
- Test Disaster Recovery Plans
- Business Continuity
- Physical Security
- Personnel Safety Concerns

Understand and Support Investigations

- Evidence Collection and Handling
- Reporting and Documenting
- Investigative Techniques
- Digital Forensics

Evidence Collection and Handling

- Evidence must be reliable. It is common during forensic and incident response investigations to analyze digital media.
- Critical to maintain the integrity of the data during the course of its acquisition and analysis
    - Checksums can ensure that no data changes occurred as a result of the acquisition and analysis. One-way hash functions such as MD5 or SHA-1 are commonly used for this purpose.
- **Chain of custody** requires that, once evidence is acquired, full documentation regarding who, what, and when and where evidence was handled be maintained

Evidence Collection and Handling

- While interviewing witnesses may seem like a straightforward process, care must be taken to avoid invalidating the process
- Interviewing is both an art and a science, and success relies on proper training, experience, and preparation
- Witnesses can be easily influenced, intimidated, and/or become uncooperative
- Properly trained and experienced personnel should conduct a witness interview.

Reporting and Documenting

- Vital to have a formal process in place to document what worked well, what did not work well, and what was totally unexpected.

Investigative Techniques

- Just like with traditional investigations, understanding the means, opportunity, and motives as well as the way the crime was committed, allows for a more thorough investigation or root cause analysis.
- Identifying the root cause correctly and quickly is extremely important when dealing with an incident, whether it is criminal or not.

Digital Forensics

- Network
  - Analysis and examination of data from network logs and network activity for use as potential evidence
- Media
  - Media analysis involves the recovery of information or evidence from information media such as hard drives, DVDs, CD-ROMs or portable memory devices
- Software
  - Software analysis or forensics refers to the analysis and examination of program code. The code being analyzed can take the form of source code, binaries, or machine code
  - Decompiling and reverse engineering techniques are often used as part of the process

Requirements for Investigation Types

- Operational
  - Concerning local/organizational policy breaches
- Criminal
  - Concerning acts against the public or state
- Civil
  - Concerning breaches of contracts or agreements
- Regulatory
  - Concerning acts against regulations (local or state)

Conduct Logging and Monitoring Activities

- Intrusion Detection and Prevention
- Security Information and Event Management (SIEM)
- Continuous Monitoring
- Egress Monitoring

Intrusion Detection and Prevention

- An IDS attempts to detect activities on the network or host that are evidence of an attack and warn administrators or incident-response personnel of the discovery, but it does not take any action on the problems found.

- An intrusion prevention system (IPS) is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity.

Security Information and Event Management

- Security Information and Event Management (SIEM) is a term used to describe a group of technologies that aggregate information about access controls and selected system activity to store for analysis and correlation
- Logs and system information may be collected for a variety of reasons

Continuous Monitoring

- Security continuous monitoring is seen as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
- Established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls

Egress Monitoring

- Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another
- It is the information flow from a private computer network to the Internet that is being monitored and controlled.
- Packets that are being sent out of the internal network are examined with a router, firewall, or similar perimeter device.
- Data Loss Prevention (DLP) is a suite of technologies aimed at stemming the loss of sensitive information that occurs in the enterprise

Secure the Provisioning of Resources

- Asset Inventory
  - Hardware and Software
- Configuration Management
- Physical Assets
- Virtual and Cloud Assets
- Applications

Understand and Apply Foundational Security Operations Concepts

- Need-to-Know/Least Privilege
- Separation of Duties and Responsibilities
- Monitor Special Privileges
- Job Rotation
- Information Lifecycle
- Service-level Agreements

Need-to-Know/Least Privilege

- Least privilege means users should be granted the minimum amount of access (authorization) required to do their jobs, but no more. Least privilege is applied to groups of objects.
- Need to know is more granular than least privilege here the user must need to know that specific piece of information before accessing it.

Need-to-Know/Least Privilege

- Access aggregation occurs as individual users gain more access to more systems. This can happen intentionally, as a function of Single Sign-On (SSO). It can also happen unintentionally where users often gain new entitlements (also called access rights) as they take on new roles or duties. This can result in authorization creep where users gain more entitlements without shedding the old ones.
- The power of these entitlements can compound over time, defeating controls such as least privilege and separation of duties.
- User entitlements must be routinely reviewed and audited.
- Processes should be developed that reduce or eliminate old entitlements as new ones are granted.

Separation of Duties and Responsibilities

- Separation of duties (also called segregation of duties) allows an organization to maintain checks and balances among the employees with privileged access.
- By having more than one individual perform part of a sensitive transaction, each person involved is supervising the other when access is granted and used.
- No one person should have total control of a sensitive transaction

Monitor Special Privileges

- Only authorized users should be granted access and for only the period of time that they require that access
- Means validating their trustworthiness and occasionally revalidating their privileges

Job Rotation

- Rotation of duties describes a process that requires different staff members to perform the same duty.
- By rotating those staff members, the organization protects itself by having these varying staff members perform and review the work of their peers who performed the same work during the last rotation.
- Rotation of duties helps mitigate collusion, where two or more people work to subvert the security of a system

Information Lifecycle

- Creation, Use, and Destruction
- When information is created, someone in the organization must be directly responsible for it. This is the individual or group that created, purchased, or acquired the information to support the mission of the organization
- During Use, it must be marked clearly for appropriate usage by authorized subjects
- Destroy data when not longer necessary. Document and have policies in place for procedures, timelines and retention requirements

Service-level Agreements

- A Service-Level Agreement (SLA) stipulates all expectations regarding the behavior of the department or organization that is responsible for providing services and the quality of the services provided.
- Usually, Service-Level Agreements will dictate what is considered acceptable regarding things such as bandwidth, uptime, time to delivery, response times, etc.

Coming Up!

- We will continue with Domain 7 starting with Resource Protection Techniques.

Employ Resource Protection Techniques

- Media Management
- Hardware and Software Asset Management

Media Management

- Media containing sensitive or confidential information should be encrypted
- Original copies of software media should be controlled through a software librarian
- Removable Media
- Archives

Hardware and Software Asset Management

- Cable Locks
- Physical Security
- Who will be the responsible party for the tracking of Hardware Assets? Security Professional? IT Manager? Maintenance or Custodial staff?

- Employ software packages that help track software/application installations and usage
  - Tracking licensing
  - Proper Access Control

Conduct Incident Management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons Learned

Detection

- Detection or identification is the phase where events are analyzed in order to determine whether they comprise a security incident.
    - An event is any auditable action on a system or network (such as a server reboot or a user logging in to check e-mail)
    - An incident is a harmful event (such as a denial of service attack that crashes a server)

Response

- Response is the phase where events are being dealt with – A plan has been formalized and action is starting

- Depending on the type of incident will depend on our response

- Containment may take place at this phase

Mitigation

- Mitigation is the phase where the Incident is being lessened
  - Triage

- Steps are being taken to remove or “fix” the issue that caused the Incident in the first place

Remediation

- Removing the root cause of the Incident

- This is our step before recovery

- We cannot recover before the “What” is removed or remediated from the system that caused the Incident

Recovery

- Recovery is the phase where we are getting the Organization back on it’s feet for production

- Recovering data; Restoring an Image; Reinstallation of software

Reporting

- Some organizations or entities are required to report Incidences; Others may not have to and can simply fix the issue

- Who will be doing the reporting?
- Where will they be reporting?
  - US-Cert
  - Stakeholders

Lessons Learned

- The goal of the lessons learned phase is to provide a final report on the incident, which will be delivered to management
- Feedback from this phase feeds directly into continued preparation, where the lessons learned are applied to improve preparation for handling future incidents

Operate and Maintain Preventative Measures

- Firewalls
- Intrusion Detection and Prevention Systems
- Whitelisting/Blacklisting
- Third-party Security Services
- Sandboxing
- Honeypots/Honeynets
- Anti-Malware

Firewalls

- Firewalls filter traffic between networks
- TCP/ IP packet filter and stateful firewalls make decisions based on Layers 3 and 4 (IP addresses and ports)
- Proxy firewalls can also make decisions based on Layers 5-7
- Firewalls are multihomed meaning they have multiple NICs connected to multiple different networks

Intrusion Detection and Prevention Systems

- An Intrusion Detection System (IDS) is a detective device designed to detect malicious (including policy-violating) actions
- An Intrusion Prevention System (IPS) is a preventive device designed to prevent malicious actions
- There are two basic types of IDSs and IPSs
  - network based
  - host based

Whitelisting/Blacklisting

- Application whitelisting is a more recent addition to endpoint security suites
- The primary focus of application whitelisting is to determine in advance which binaries are considered safe to execute on a given system
- Once this baseline has been established, any binary attempting to run that is not on the list of known-good binaries is prevented from executing
- Blacklisting the same but DENYING execution

Third-party Security Services

- Contract with a third-party company to help provide

- Comprehensive fuzz testing

- Testing mobile and cloud-based applications

Sandboxing

- A sandbox segregates the code from the operating system.
- The sandbox is designed to prevent an attacker who is able to compromise from accessing system files, such as the password file

Honeypots/Honeynets

- Honeypot systems are decoy servers or systems set up to gather information regarding an attacker or intruder into your system
- Honeypots can be set up inside, outside, or in the DMZ of a firewall design or even in all of the locations
- Honeynets are a collection of honeypots

Anti-Malware

- Anti-malware is a software program designed to prevent, detect and remediate malicious programming
- Anti-malware software protects against infections caused by many types of malware, including viruses,worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware
- Anti-malware software can be installed on an individual computing device, gateway server or dedicated network appliance
- It can also be purchased as a cloud service or be embedded in a computing device's firmware

Patch and Vulnerability Management

- The term vulnerability management is used rather than just vulnerability scanning to emphasize the need for management of the vulnerability information
- The remediation or mitigation of vulnerabilities should be prioritized based on both risk to the organization and ease of remediation procedures
- Security baselining is the process of capturing a point in time understanding of the current system security configuration

Change Management Process

- The purpose of the change control process is to understand, communicate, and document any changes with the primary goal of being able to understand, control, and avoid direct or indirect negative impact that the change might impose

Change Management Process - Generic

- Identifying a change
- Proposing a change
- Assessing the risk associated with the change
- Testing the change
- Scheduling the change
- Notifying impacted parties of the change
- Implementing the change
- Reporting results of the change implementation

Coming Up!!

- Next we will continue on with Domain 7 starting with Recovery Strategies.

Recovery Strategies

- Backup Storage Strategies
- Recovery Site Strategies
- Multiple Processing Sites
- System Resilience, High Availability, Quality of Service and Fault Tolerance

Backup Storage Strategies

- Offsite Storage
- Electronic Vaulting
- Tape Rotation and procedures
- Full / Differential / Incremental

Recovery Site Strategies

- A hot site is a location that an organization may relocate to following a major disruption or disaster.
- The hot site will have all necessary hardware and critical applications data mirrored in real time. A hot site will have the capability to allow the organization to resume critical operations within a very short period of time

Recovery Site Strategies

- A warm site has some aspects of a hot site
- Readily accessible hardware and connectivity, but it will have to rely upon backup data in order to reconstitute a system after a disruption

Recovery Site Strategies

- A cold site is the least expensive recovery solution to implement. It does not include backup copies of data nor does it contain any immediately available hardware
- After a disruptive event, a cold site will take the longest amount of time of all recovery solutions to implement and restore critical IT services for the organization

Multiple Processing Sites

- Multiple sites spread out across the globe, nation or region

- Multiple processing sites can be an advantage if numerous locations are required to conduct business

System Resilience, High Availability, Quality of Service and Fault Tolerance

- Planning ahead
  - For an organization to be able to continually provide operational availability, they must be implemented with fault tolerance in mind.

- Redundant hardware

System Resilience, High Availability, Quality of Service and Fault Tolerance

- **RAID 0**—A RAID 0 configuration, also known as a striped set, is a configuration that relies on striping data across multiple disks. In a RAID 0 configuration, data are striped across multiple disks but no parity information is included. As a result, although performance is improved, RAID 0 provides no data redundancy. Because no redundancy is provided by a RAID 0 configuration, it is not a viable solution for disaster recovery.
- **RAID 1**—In a RAID 1 configuration, data mirroring is used. Identical copies of data are stored on two separate drives. In the event that one disk fails, an exact duplicate of the data resides on the other disk. RAID 1 is a simple solution to implement; however, 50% of total disk space is lost because all data are duplicated on both disks.

System Resilience, High Availability, Quality of Service and Fault Tolerance

- **RAID 2**—In a RAID 2 configuration, striping is performed at the bit level. RAID 2 configuration is costly, difficult to implement and, therefore, not used in practice.
- **RAID 3**—In a RAID 3 configuration, striping is performed at the byte level and uses a dedicated parity disk. RAID 3 is not used in practice.
- **RAID 4**—RAID 4 configurations implement striping at the block level and uses a dedicated parity disk. RAID 4 is not used in practice.

System Resilience, High Availability, Quality of Service and Fault Tolerance

- **RAID 5**—RAID 5 uses block level striping with parity information that is distributed across multiple disks. In the event that a single disk fails, the data on the disk can be recreated based on the data that are stored on the remaining disks.

Disaster Recovery Processes

- Response
- Personnel
- Communications
- Assessment
- Restoration
- Training and Awareness

Response

- In order to begin the disaster recovery process, there must be an initial response that begins the process of assessing the damage. Speed is essential during this initial assessment
- The initial assessment will determine if the event in question constitutes a disaster

Personnel

- If a disaster is declared, then the recovery team needs to be activated.
- Depending on the scope of the disaster, this communication could prove extremely difficult.
- The use of calling trees, should help to facilitate this process to ensure that members can be activated as smoothly as possible.

Communications

- One of the most difficult aspects of disaster recovery is ensuring that consistent timely status updates are communicated back to the central team managing the response and recovery process
- The typical communication method of leveraging an office phone will quite often not be a viable option
- In addition to communication of internal status regarding the recovery activities, the organization must be prepared to provide external communications, which involve disseminating details regarding the organization's recovery status with the public.

Assessment

- Though an initial assessment was carried out during the initial response portion of the disaster recovery process, a more detailed and thorough assessment will be performed by the disaster recovery team.
- The team will proceed to assessing the extent of the damage to determine the proper steps necessary to ensure the organization's ability to meet its mission.

Restoration

- The primary goal of the reconstitution phase is to successfully recover critical business operations at either primary or secondary site
- If an alternate site is leveraged, adequate safety and security controls must be in place in order to maintain the expected degree of security the organization typically employs
- The use of an alternate computing facility for recovery should not expose the organization to further security incidents.

Training and Awareness

- Although there is an element of DRP training that comes as part of performing the tests there is a need for more detailed training on some specific elements of the DRP process
  - Power switch over
  - Data switch over
  - Call Trees
- Another aspect of training is to ensure adequate representation on staff of those trained in basic first aid and CPR.

Test Disaster Recovery Plans

- Read-Through
- Walk-Through
- Simulation
- Parallel
- Full Interruption

Read-Through

- Checking for all necessary components required for successful recovery and ensures that they are, or will be, readily available should a disaster occur.
- Test is focused on ensuring that the organization has, or can acquire in a timely fashion, sufficient level resources on which their successful recovery is dependent

Walk-Through

- Another test that is commonly completed at the same time as the Read-Through test is the structured walk-through
- The goal is to allow individuals who are knowledgeable about the systems and services targeted for recovery to thoroughly review the overall approach
- The group will talk through the proposed recovery procedures in a structured manner to determine whether there are any noticeable omissions, gaps, erroneous assumptions, or simply technical missteps that would cause issues for the recovery process from successfully occurring

Simulation

- A simulation test goes beyond talking about the process and actually has teams to carry out the recovery process
- A pretend disaster is simulated to which the team must respond as they are directed to by the DRP

- The goal of any testing of a DRP is to help ensure that the organization is well prepared in the event of an actual disaster

Parallel

- Another type of DRP test is that of parallel processing. This type of test is common in environments where transactional data is a key component of the critical business processing
- Typically, this test will involve recovery of critical processing components at an alternate computing facility and then restore data from a previous backup
- This is done without disrupting the production site or data

Full Interruption

- Arguably, the most high fidelity of all DRP tests involves business interruption testing
- However, this type of test can actually be the cause of a disaster, so extreme caution should be exercised before attempting an actual interruption test
- The business interruption style of testing will have the organization actually stop processing normal business at the primary location but will instead leverage the alternate computing facility
- These types of tests are more common in organizations where fully redundant, often load-balanced, operations already exist.

Business Continuity Planning and Exercises

- Business Continuity Planning (BCP) and Disaster Recovery Planning are two distinct disciplines.
- The goal of a BCP is for ensuring that the business will continue to operate before, throughout, and after a disaster event is experienced
- The focus of a BCP is on the business as a whole and ensuring that those critical services that the business provides or critical functions that the business regularly performs can still be carried out both

Physical Security

- Perimeter
- Internal Security

Perimeter

- Perimeter defenses help prevent, detect, and correct unauthorized physical access. Buildings should employ defense in depth just like networks
- Any one defense may fail, so critical assets should be protected by multiple physical security controls, such as fences, doors, walls, locks, etc…
- The ideal perimeter defense is safe, prevents unauthorized ingress, and, when applicable, offers both authentication and accountability.

Internal Security

- Motion Sensors
- Cameras
    - Hidden
    - Motion detection
    - Plan view
- Escorting Visitors
    - Visitors are given temporary badges, but this badge does not double as an access card
- Man Traps
- Turnstiles
- Electronic/Magnetic Locks
- Vaults
- Key Control/Management

Participate in Addressing Personnel Safety Concerns

- Privacy
    - Do they have it?

- Travel
    - Customs in other countries
    - Threats abroad

- Duress
    - Threatened for non-compliance (bank teller, cancelling an alarm, etc…)
    - Training and Preparedness

Domain 7 Complete!!

- Investigations
- Requirements for Investigation Types
- Logging and Monitoring Activities
- Provisioning of Resources
- Foundational Security Operations Concepts
- Resource Protection Techniques
- Incident Management
- Preventative Measures

Domain 7 Complete!!

- Path and Vulnerability Management
- Change Management
- Recovery Strategies
- Disaster Recovery Process
- Test Disaster Recovery Plans
- Business Continuity
- Physical Security
- Personnel Safety Concerns

*

CISSP

Domain 8

Software Development Security

(Understanding, Applying and Enforcing Software Security)

Some Key Areas

- Software Development Lifecycle (SDLC)
- Development Environments
- Software Security
- Acquired Software

Software Development Lifecycle (SDLC)

- Development Methodologies
- Maturity Models
- Operation and Maintenance
- Change Management
- Integrated Product Team

Software Development Lifecycle (SDLC)

- Provides a framework for the phases of a software development project from defining the functional requirements to implementation.
- The model chosen should be based on the project
- Three basic phases
  - Concept
  - Design
  - Implement

Development Methodologies - Waterfall

- Each phase is completed in sequence (consecutively) and contains a list of activities that must be performed before the next phase begins

Development Methodologies - Spiral Method

- Each phase adds a risk assessment review
- Schedules and estimated costs to complete are revised each time the risk assessment is performed
- The decision as to whether to continue or to cancel the project is made based on the results of each of these risk assessments

Development Methodologies - Rapid Application Development (RAD)

- RAD is a form of rapid prototyping that requires strict time limits on each phase and relies on tools that enable quick development
- This may be a disadvantage if decisions are made so rapidly that it leads to poor design

Development Methodologies - Agile Development

- A description of development with short development iterations to reduce risk
- Like extreme programming, agile requires highly skilled small teams that are designing, developing, and testing their work in small functional components and through continuous review ensuring that it is working correctly

Maturity Models

- Software Engineering Institute
  - Capability Maturity Model for Software
  - 5 steps or maturity levels for development
    - Initial level
    - Repeatable level
    - Defined level
    - Managed level
    - Optimized level

Capability Maturity Model for Software

- At the *initial* level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.
- At the *repeatable* level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.
- At the *defined* level, an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
- At the *managed* level, an organization monitors and controls its own processes through data collection and analysis.
- At the *optimizing* level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

Operation and Management

- In Operation and Management we are actually using the software that has been developed
- Also involves monitoring the performance of the system and ensuring continuity of operations.
- From a security standpoint we will include testing backup and recovery procedures, ensuring proper controls for data and report handling, and ensuring the effectiveness of security processes

Change Management

- Primary objective is to enable beneficial changes to be made, with minimal disruption to IT services.
- Ensures changes are deployed in a controlled way

Basic Concepts

- Request for Change (RFC)
    - Formal request to change one or more CIs
        - May be proceeded by a Change Proposal
    - 3 types of change request
        - Normal Change
            - Addition, modification or elimination of anything that could have an effect on IT Services
        - Standard Change
            - Pre-approved, low-risk and relatively common change
                - Change model used -> steps to perform the change
        - Emergency Change
            - Introduced as soon as possible

Basic Concepts

- Change Advisory Board (CAB)
  - Body or group that meets to help the change manager/authority to assess, prioritize and schedule the changes

- Post-Implementation Review (PIR)
  - Determines if the change was successful and to identify opportunities for improvement

Change Management

- Create and Record the RFC
  - All RFCs are registered and must be identifiable
- Review the RFC
  - Is it illogical, unfeasible unnecessary or incomplete or has it already been submitted
- Assess and evaluate the change
  - Is the change moving forward?
- Authorize the Change Build and Test
  - We're a go

Change Management

- Coordinate Change Build and Test
  - Technical groups have for building the changes
- Authorize Change Deployment
  - Proof that the result of the change was properly built and tested. Formal report
- Coordinate Change Deployment
  - Part of the Release and Deployment Management process. Remediation procedures should be prepared and documented in advance

Change Management

- Review and Close Change Record
    - Deployed changes are evaluated after some time period, if successful can be finalized and closed.

Integrated Product Team (IPT)

- When it comes to product development, working in teams has proven to be more effective and overall better for the organization
  - These teams usually report to some Team Lead
- Better input and multiple ideas, opinions, identify and resolve issues, and make sound and timely decisions

- DevOps approach includes lines of business, practitioners, executives, partners, suppliers.
  - Practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support

Vulnerabilities at the source-code level

- **Hard-coded credentials**: Backdoor username/ passwords left by programmers in production code
- **Buffer overflow**: Occurs when a programmer does not perform variable bounds checking
- **SQL injection**: Manipulation of a back-end SQL server via a front-end Web server
- **Directory path traversal**: Escaping from the root of a Web server (such as/ var/ www) into the regular file system by referencing directories such as “../..”
- **Cross-Site Scripting (XSS):** Third-party injection of a script into a Web page within the security context of a trusted site
- **Cross-Site Request Forgery (CSRF):** Third-party submission of predictable content to a Web application within the security context of an authenticated user

Privilege escalation

- Privilege escalation vulnerabilities allow an attacker with (typically limited) access to be able to access additional resources
- Improper software configurations and poor coding and testing practices often cause privilege escalation vulnerabilities

Coming Up!

- Next we will continue on with Domain 8 starting with a refresher on Databases.

Database Security

- A database is a structured collection of related data.
- Databases allow queries, insertions, deletions, and many other functions.
- The database is managed by the Database Management System (DBMS), which controls all access to the database and enforces the database security.
- Databases are managed by Database Administrators (DBAs).

Database Security

- Databases may be searched with a database query language, such as the Structured Query Language (SQL)
- Typical database security issues include the confidentiality and integrity of the stored data. Integrity is a primary concern when replicated databases are updated.

Configuration Management

- Monitoring and managing changes to a program or documentation.
- The goal is to guarantee integrity, availability, and usage of the correct version of all system components such as the software code, design documents, documentation, and control files
- Reviewing every change made to a system.
    - Identifying, controlling, accounting for, and auditing all changes
- Intended to eliminate the confusion and error brought about by the existence of different versions of documentation, hardware or software

Code Repositories

- Is our code secure?
- Where is located?
- Who has access to the data?

- While researching for ideas came across GitHub’s Code Repository security and it really paints a great picture of secure repositories

GitHub’s Code Repository security

- **Physical Security**
- Data center access limited to data center technicians and approved GitHub staff
- Biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- 24x7 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities to help maintain low profile
- Physical security audited by an independent firm

GitHub’s Code Repository security

- **System Security**
- System installation using hardened, patched OS
- Dedicated firewall and VPN services to help block unauthorized system access
- Distributed Denial of Service (DDoS) mitigation services powered by industry-leading solutions

GitHub’s Code Repository security

- **Operational Security**
- Our primary data center operations are regularly audited by independent firms against an ISAE 3000/AT 101 Type 2 Examination standard
- Systems access logged and tracked for auditing purposes
- Secure document-destruction policies for all sensitive information
- Fully documented change-management procedures

GitHub’s Code Repository security

- **Software Security**
- We employ a team of 24/7/365 server specialists at GitHub to keep our software and its dependencies up to date eliminating potential security vulnerabilities. We employ a wide range of monitoring solutions for preventing and eliminating attacks to the site.

GitHub’s Code Repository security

- **Communications**
- All private data exchanged with GitHub is always transmitted over SSL. All pushing and pulling of private data is done over SSH authenticated with keys, or over HTTPS using your GitHub username and password.
- The SSH login credentials used to push and pull can not be used to access a shell or the filesystem. All users are virtual (meaning they have no user account on our machines) and are access controlled through the peer reviewed, open source git-shell.

GitHub’s Code Repository security

- **File system and backups**
- Every piece of hardware we use has an identical copy ready and waiting for an immediate hot-swap in case of hardware or software failure. Every line of code we store is saved on a minimum of three different servers, including an off-site backup.

GitHub’s Code Repository security

- **Employee access**
- No GitHub employees ever access private repositories unless required to for support reasons. Staff working directly in the file store access the compressed Git database, your code is never present as plaintext files like it would be in a local clone. Support staff may sign into your account to access settings related to your support issue. In rare cases staff may need to pull a clone of your code, this will only be done with your consent.

GitHub’s Code Repository security

- We protect your login from brute force attacks with rate limiting. All passwords are filtered from all our logs and are one-way encrypted in the database
- Login information is always sent over SSL.
- We also allow you to use two-factor authentication as an additional security measure when accessing your GitHub account

GitHub’s Code Repository security

- **Credit card safety**
- When you sign up for a paid account on GitHub, we do not store any of your card information on our servers. It's handed off to third party, a company dedicated to storing your sensitive data on PCI-Compliant servers

Application Programming Interface - API

- Application Programming Interfaces are the connectors for the Internet of Things (IoT), allowing our devices to speak to each other
- APIs are plagued with security problems
- The problem is usually not the concept behind the API but rather how it is coded. Many application developers are failing to write or use APIs with security in mind, putting both the application and the underlying data at risk
- Vulnerability, Penetration Tests, Fuzzing and Manual code review are ways to help mitigate most API issues

Access the Effectiveness of Security Software

- Auditing and Logging of changes
- Risk Analysis and Mitigation
- Acceptance Testing

Auditing and Logging of changes

- Logs are the primary record keepers of system and network activity.
- When security controls experience failures, logs are particularly helpful in capturing the pertinent information that will help the security professional understand what has happened and why

Risk Analysis and Mitigation

- Risk is defined as an event that has a probability of occurring
- All projects assume some element of risk, and it is through risk management where tools and techniques are applied to monitor and track those events that have the potential to impact the outcome of a project.
- Risk management is an ongoing process that continues through the life of a project.
- Mitigation is to lesson our risk

Acceptance Testing

- Acceptance testing is a formal test conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system.
- Can be designed by the customer
- Usually tests an exact or very near exact replicate of the environment it is intended for

Acquired Software

- Ensure that a well-documented Software Assurance policy and process is in place in the enterprise

- US-Cert phases
  - Planning Phase
  - Monitoring and Acceptance Phase
  - Follow-on Phase

Planning Phase

- Needs determination for acquiring software services or products, identifying potential alternative software approaches, and identifying risks associated with those alternatives.
- Developing software requirements to be included in work statements
- Creating an acquisition strategy and/ or plan that includes identifying risks associated with various software acquisition strategies
- Developing evaluation criteria and an evaluation plan.

Monitoring and Acceptance Phase

- This phase involves monitoring the supplier's work and accepting the final service or product delivered under a contract. This phase includes three major activities:
  - Establishing and consenting to the contract work schedule
  - Implementing change (or configuration) control procedures
  - Reviewing and accepting software deliverables.

Follow-on

- This phase involves maintaining the software
    - Sustainment (includes risk management, assurance case management, and change management)
    - Disposal or decommissioning
    - During the follow-on phase, software risks must be managed through continued analysis of the assurance case and should be adjusted to mitigate changing risks

Domain 8 Complete!

- Software Development Lifecycle (SDLC)
- Development Environments
- Software Security
- Acquired Software