CISSP Notes

CIA Triad

- Confidentiality
    - Resources should be protected from unauthorized access
    - Prioritized by governments
    - Concepts
        - Sensitivity
            - How harmful is disclosure
        - Discretion
            - Controlled disclosure to prevent damage
        - Criticality
            - How essential the information is to the organization?
        - Concealment
            - Hiding information (e.g. obfuscation)
        - Secrecy
            - Keeping something a secret
        - Privacy
            - Keeping personal information secret
        - Seclusion
            - Storing data in out-of-the-way locations
        - Isolation
            - Keeping data separate
- Integrity
    - Resources should be protected from unauthorized modification
    - Resources should maintain semantic consistency
- Availability
    - Resource should be accessible to authorized parties
    - Prioritized by businesses

AAA

- Required to hold a subject accountable for actions
- Identification
    - Subject identifies themselves
- Authentication
    - Subject proves their identity
- Authorization

  - Subject is allowed/disallowed to perform an action
  - What can the subject do and not do?
- Auditing
  - Subject's actions are logged
- Accounting
  - Subject's logs are reviewed for violations
  - Subject is held accountable for their actions
  - Legally Defensible Security
    - Required to hold subjects accountable
    - You need to prove:
      - Efforts were made to prevent the crime
      - Log files are accurate
      - All laws and regulations were followed
      - Warning and notifications were posted
      - Electronic evidence is decisive
  - Non-repudiation
    - Subjects cannot deny performing an action

Protection Mechanism

- Layering/Defense-in-Depth
  - Use of multiple controls in a series
  - Uses series vs. parallel
    - Series
      - Useful for security
      - Data passes through multiple filters
      - Airport with multiple gates
    - Parallel
      - Useful for performance
      - Data can pass any filter
      - Mall with multiple entrances
- Abstraction
  - Generalizes a group of objects and subject
  - Defines object and subject templates
  - E.g. "Employee" can be used to describe "Linda", "Mark", etc.
- Data Hiding
  - Places data in location not seen by subject
  - Prevents data from being accessed by unauthorized subjects
- Encryption
  - Hides intent of data rather than hiding the data itself

    - Makes data unreadable to unauthorized subjects

Security Governance

- Administration of an organization's security program
- Business Case
    - Justifies starting a new project
- Approaches
    - Top-down
        - Upper management makes security policies
        - Lower professionals flesh out security policies
    - Bottom-up
        - IT staff makes security decisions
        - Problematic
- Autonomous InfoSec Team
    - Led by the CSO
    - Reports directly to senior management
- Security Policy
    - Requires support of senior management to succeed
    - Evidence of due care and due diligence

Security Management Plans

- Strategic Plan
    - Long-term plan
    - Defines security purpose of organization
    - Lifetime: 5 years
- Tactical Plan
    - Mid-term plan
    - Contains TASKS to achieve Strategic Plan
    - Examples
        - Project plans
        - Acquisition plans
        - Hiring plans
        - Budget plans
    - Lifetime: 1 year
- Operation Plan
    - Short-term plan
    - Contains STEPS to achieve Tactical Plan

    - Examples
        - Training plans
        - System deployment plans
        - Product design plans
    - Lifetime: 1 month/1 quarter

Change Management

- Changes can lead to security issues
- Purpose
    - Prevents compromise after change
- Goals
    - Monitor change
    - Test change
    - Allow rollback of change
    - Inform users of change
    - Analyze effects of change
    - Minimize negative impact of change
    - Allow review of change by Change Approval Board (CAB)

Data Classification

- Identify which data need to be prioritized for protection
- Identify which controls is needed for which data
- Benefits
    - Demonstrates commitment to protection of data
    - Identifies critical assets
    - Justifies selection of controls
    - Required for regulations
    - Defines proper access, declassification, and destruction method
    - Helps with data life-cycle management
- Classification Criteria's
    - Usefulness
    - Timeliness
    - Value
    - Age
    - Lifetime
    - Relationship with subjects

    - Sensitivity
    - Criticality
    - National Security Implications
    - Storage method
    - Ownership
- Implementing Classification
    - Identify custodian
    - Determine evaluation criteria
    - Classify resources
    - Determine exceptions
    - Determine security controls
    - Determine declassification procedure
    - Staff awareness/training
- Classification Schemes
    - Government/Military
        - Classified
            - Top Secret
            - Secret
            - Confidential
        - Unclassified
            - Sensitive
            - Unclassified
    - Private/Business
        - Confidential/Private
            - Confidential/Proprietary: Related to business
            - Private: Related to personnel
        - Sensitive
        - Public

Security Roles and Responsibilities

- Roles and Responsibilities
    - Senior Manager
        - Signs off on policy issues
        - Liable for security solution
    - Security Professional
        - Designs and implements security solutions
    - Data Owner
        - Classifies data
    - Data Custodian

        - Implements controls to protect data
        - Protects data based on classification
    - User
        - Accesses the system
        - Complies with security policies
    - Auditor
        - Checks for compliance to security policy
        - Checks effectiveness of security policy
- Training vs Education
    - Training
        - So users can comply with security policies
    - Education
        - Users lean more than what they need to know

Control Frameworks

- For planning IT security of an organization
- Control Objectives for Information and Related Technology (COBIT)
    - By ISACA
    - Principles
        - Meeting Stakeholder Needs
        - Covering the Enterprise End-to-End
        - Applying a Single Integrated Framework
        - Enabling a Holistic Approach
        - Separating Governance from Management

Due Care and Due Diligence

- Due Care
    - Required effort to protect data
    - Compliance to legal regulations
    - Legal duty of company
    - Failure will result in negligence
- Due Diligence
    - Maintaining due care
    - Continuous improvement of security
    - Penetration tests, vulnerability assessments, etc.
- Operational Security
    - Ongoing maintenance of due care and due diligence

Components of Security Policies

- Should be kept as separate documents
  - Only changed materials need to be redistributed
  - Not all users are concerned with all documents
- Security Policy
  - Generalization of security needs, goals, and practices
  - Broad overview of security
  - Strategic plan
  - Proof of due care
  - Compulsory
  - Responsibilities must be roles-based, not individual-based
  - Types
    - Organizational
    - Issue-specific
      - Network Service
      - Department
    - System-specific
  - Categories
    - Regulatory
      - Required by law
    - Advisory
      - Required by senior management
      - Acceptable Use Policy
        - Assigns security roles
        - Assigns responsibilities to roles
        - Contains expected behavior
    - Informative
      - Not required
      - Provides background information to issues
- Standard
  - Describes uniform implementation of technology
  - Tactical documents
- Baselines
  - Describes a secure state for a system
  - System-specific
- Guideline
  - Recommendations and suggested actions for compliance
  - Describes controls rather than products
  - Not compulsory

- Procedure
    - Step-by-step instruction on how to implement a security control
    - Specific to a system or product
    - Ensures compliance to standard

Threat Modeling

- Approaches
    - Proactive
        - Performed before and while the system is being implemented
        - Predicting threats and designing defenses in advance
        - More cost effective and more successful
        - Security Development Lifecycle
            - Reduce number of coding defects
            - Reduce severity of remaining defects
    - Reactive
        - Performed after the system has been implemented
        - Less effective but more cost effective than redesign
        - E.g. penetration testing, source code review, fuzz testing
        - Fuzz Testing
            - Random invalid input is fed to a program
            - Attempts to find previously undetected flaws
- Steps
    - Threat Identification
        - Approaches
            - Focused on Assets
                - Protect valuable assets
            - Focused on Attackers
                - Protect the things that attackers want to attack
            - Focused on Software
                - Protect the software
        - Individual Threats
            - Be cautious of
                - Contractors
                - Trusted Partners
    - Threat Categorization
        - STRIDE
            - Spoofing
                - Falsifying information to gain access
            - Tampering
                - Making unauthorized changes

- Repudiation
  - Denying having done an action
- Information Disclosure
  - Revelation of controlled information
- Denial-of-Service
  - Prevents the use of an asset
- Escalation of Privilege
  - Elevates capability of under privileged account

- Determining Potential Attacks
  - Data Flow Diagrams
    - Entities
    - Technologies
    - Transactions
    - Attacks vs each element
- Reduction Analysis
  - Decomposing system/process/environment
    - Modules
    - Functions
    - Protocols
    - etc.
  - Identify the Following
    - Trust Boundaries
    - Data Flow Paths
    - Input Points
    - Privileged Operations
    - Security Approach
- Prioritization and Response
  - Probability x Damage Potential
  - High/Medium/Low
  - DREAD
    - Discoverability
    - Reproducibility
    - Exploitability
    - Affected Users
    - Damage Potential

Acquisition Security

- Select software with integrated security
- Evaluate 3rd party service provider

    - On-Site Assessment
        - Observe their operating habits
    - Document Exchange and Review
        - Investigate data exchange process
    - Process/Policy Review
        - Review their security policy
- Review Service Level Agreements

Personnel Security

- People
    - Weakest link in security chain
- Hiring Process
    - Job Description
        - Concepts
            - Separation of Duties
            - Least Privilege
            - Job Responsibilities
            - Job Rotation
            - Cross-training
        - Maintain throughout organization lifecycle
    - Job Classification
    - Employee Screening
        - Background checks, etc.
    - Hiring and Training
        - Non-disclosure Agreement
        - Non-compete Agreement
    - Termination
        - Notify employee
        - Request return of company equipment
        - Disable electronic access
        - Exit interview and NDA review
        - Escort off premises
- Separation of Duties
    - Work tasks divided among administrators
    - Applies to administrators instead of users
    - Prevents collusion
- Least Privilege
    - Users should only have privileges that they require
    - Applies to users instead of admins

- Job Responsibilities
  - Work tasks that an employee is required to perform
  - Defines required objects, resources, and services
- Job Rotation
  - Provides knowledge redundancy
  - Less downtime
  - Reduces risk of fraud via peer auditing
  - Protects against collusion
- Cross-training
  - Alternative to job rotation
  - Employees are trained for other jobs
  - Workers are not rotated through different job
- Collusion
  - When people work together to commit a crime
- Non-disclosure Agreement (NDA)
  - Protects confidential information within an organization
- Non-compete Agreement (NCA)
  - Prevents employees from jumping to a competitor
  - Has time limit
  - Allows company to keep competitive edge
  - Difficult to enforce
  - Deters violation of NDA
- Mandatory Vacations
  - Used to audit employees
- Termination Best Practices
  - Have one witness
  - Escort off premises
  - Escort required when in work area
  - Return employee identification and equipment
  - Disable network user account at same time of termination
  - Notify HR to issue final paychecks
  - Inform security personnel of termination
  - Terminate at end of shift in middle of week
  - Perform exit interview
- Exit Interview
  - Review liabilities and restrictions
  - Review NDA and other agreements
- Third-party Controls
  - Service Level Agreements
    - Defines expected level of service from third-party

        - Put in place for network connections and services
        - Includes remedies if not met
        - Common SLA Issues
            - System uptime
            - Maximum consecutive downtime
            - Peak load
            - Average load
            - Responsibility for diagnostics
            - Failover time
- Compliance
    - Adherence to regulations
    - Employees need to follow polices, etc.
- Privacy
    - Secrecy of personal information
    - Prevention of unauthorized access to PII
    - Freedom from being monitored without knowledge
    - For employees, site visitors, customers, suppliers, and contractors
- Personally Identifiable Information
    - Information that can be traced back to a person
    - Includes
        - Phone
        - Email
        - Address
        - SSN
        - Name
    - Excludes
        - MAC Address
        - IP Address
        - OS Type

Security Governance

- Directing the security efforts of an organization
- Third-party Governance
    - Employment of external auditors
        - External auditors review your security
    - Compliance of external providers
        - Providers must comply with your security policies
        - Documentation Review

- On-site assessments

- Documentation review
  - Exchanging materials
  - Reading and verifying them against expectations
  - Required before preforming on-site assessments
- On-site assessments
  - First hand exposure to security mechanisms
  - Auditors should follow COBIT
- Authorization to Operate (ATO)
  - For government contractors
  - Required when complying with government security policies

Risk Management

- Risk
  - Possibility that assets could be damaged or disclosed
- Risk Management
  - Actions to reduce risk to an acceptable level
  - Steps
    - Risk Analysis
      - Identify
      - Evaluate
      - Countermeasures
    - Risk Responses
      - Mitigate
        - Using countermeasures to reduce risk
      - Transfer
        - Transferring risk to another organization
        - Purchasing insurance
        - Outsourcing business processes
      - Accept
        - When countermeasure costs more than risk cost
        - Organization absorbs risk cost
        - Signed off by management
      - Reject
        - Ignoring the existence of the risk
        - Not prudent due-care responses to risk
    - Countermeasure Selection and Implementation
      - Rules
        - Countermeasure Cost < Asset Value

        - Countermeasure Cost < Countermeasure Benefit
        - Benefit of Attack < Cost of Attack
        - Secure by design
        - Benefit should be testable and verifiable
    - Monitoring and Measurement
    - Continuous Improvement
- Risk Analysis
  - Process of achieving risk management goals
  - Steps
    - Identifying risk
    - Evaluating risk
      - Likelihood
      - Damage Potential
      - Risk Rating
    - Determining countermeasures
      - Cost/benefit analysis
  - Types
    - Quantitative
    - Qualitative
    - Hybrid
  - Quantitative Risk Analysis
    - Assigning dollar value to risks
    - Steps
      - Identify assets and value (AV)
      - Identify threats against assets and exposure factor (EF)
      - Determine single loss expectancy (SLE)
      - Identify annual rate of occurrence (ARO)
      - Determine annual loss expectancy (ALE)
      - Identify countermeasures and changes to ARO and ALE if applied
      - Determine countermeasure cost and benefit (Raw ALE - Controlled ALE - Annual Control Cost)
    - Values
      - Asset Value (AV)
        - The value of an asset
      - Exposure Factor (EF)
        - Percentage of loss to an asset if a risk to it is realized
      - Single Loss Expectancy (SLE)
        - Cost if a risk is realized
        - SLE = AV * EF
      - Annualized Rate of Occurrence (ARO)

        - Number of times a risk is realized per year
        - Historical records, statistical analysis, guesswork
        - Determined through Probability Determination
        - ARO = Threat Sources * Single Likelihood
      - Annualized Loss Expectancy (ALE)
        - Expected yearly cost of a risk
        - ALE = ARO * SLE
      - Annualized Loss Expectancy with Safeguard (ALE)
        - When safeguard is applied, ARO and EF changes
        - Recalculate ALE with modified ARO
        - ALE = ARO * SLE
      - Annualized Cost of Safeguard (ACS)
        - Yearly cost to implement safeguard
        - Safeguard cost should be less than asset value
        - If asset value is less than safeguard, just accept the risk
      - Safeguard Benefit
        - The amount of money saved by implementing the safeguard
        - Benefit = ALE w/o safeguard - ALE w/ safeguard - ACS
  - Qualitative Risk Analysis
    - Scenario-based
    - Uses threat-ranking
    - Techniques
      - Delphi Technique
      - Brainstorming
      - Surveys
      - etc.
    - Scenarios
      - One page description of a threat
      - Contains
        - Threat Vectors
        - Impact
        - Safeguards
        - Threat Level
    - Delphi Technique
      - Anonymous feedback-response process
      - For reaching a consensus
      - For honest feedback from participants
- Risk Terminology
  - Asset
    - Items that have value to the organization

    - Items that will damage of organization of disclosed
    - Any item that needs to be protected
  - Asset Valuation
    - Monetary or intangible value of asset
    - Can be based on cost to develop or replace, market value, etc.
  - Threats
    - Undesirable occurrences that can damage assets
  - Threat Agents
    - Sources of threats
  - Exposure
    - Possibility of threat realization
    - Exposure is equivalent to risk
  - Risk
    - Possibility of threat realization
    - risk = threat * vulnerability
  - Safeguards / Countermeasure
    - Things or acts that reduce a threat or vulnerability
    - Safeguard
      - Pro-active controls
    - Countermeasure
      - Reactive controls
  - Attack
    - Exploitation of vulnerability by threat agent
    - Intentional attempt to exploit
  - Breach
    - Occurrence of security mechanism bypass
  - Penetration
    - State where threat agent has access to organization's infrastructure
  - Total Risk
    - Risk that organization faces without safeguards
    - Total Risk = Threat * Vulnerabilities
  - Residual Risk
    - Risk that remains after countermeasures are implemented
    - Risk that management has chosen to accept
    - Residual Risk = Total Risk - Control Gap
    - Control Gap: Amount of risk reduced by controls
- Risk Elements
  - Threat exploits...
  - Vulnerability, resulting in...
  - Exposure, which is...

    - Risk, which is mitigated by…
    - Safeguards which protected…
    - Assets which are endangered by…
- Identifying Threats
    - Listing down all threat agents and events
    - Should involve various departments
    - Employment of external consultants
- Countermeasure Selection and Implementation
    - Categories
        - Technical
            - Hardware or software mechanisms
            - Firewalls, IDSs, etc.
        - Administrative
            - Policies and procedures
            - Management controls
        - Physical
            - Physically tangible
            - Guards, fences, CCTV, etc.
    - Types
        - Deterrent
            - Discourages violation of security policy
            - Fences, trainings, guards, etc.
        - Preventive
            - Stops violations of security policies
            - Firewalls, IPS, mantraps, etc.
        - Detective
            - Discovers violations of security policies
            - CCTV, audit trails, motion detectors, etc.
        - Compensating
            - Added in addition to other security controls
            - Encryption of PII at rest and in transit
        - Corrective
            - Return system to secure state after violation of policy
            - Terminating malicious activity, patching software, etc.
        - Recovery
            - Extension of corrective controls, but more advanced
            - Backups, fault tolerance, shadowing, clustering, etc.
        - Directive
            - Directs the actions of subjects
            - Notifications, escape route signs, procedures, etc.

- Asset Valuation
    - Assigning dollar value to assets
    - Factors
        - Acquisition/Development Cost
        - Management Cost
        - Maintenance Cost
        - Cost to Protect
        - Value to Owners and Users
        - Value to Competitors
        - Intellectual Property
        - Market Value
        - Replacement Cost
        - Productivity Enhancement
        - Operational Cost
        - Liability of Asset Loss
        - Usefulness
- Risk Management Framework (NIST 800-37)
    - Categorize
        - Categorize information system elements
        - Based on impact analysis
    - Select
        - Select initial security controls
    - Implement
        - Implement selected security controls
    - Asses
        - Check if controls are appropriate
        - Check if controls are implemented correctly
    - Authorize
        - Authorize operation of information system
        - Acceptance of risks
    - Monitor
        - Monitor effectiveness of controls

Education, Awareness, and Training

- Humans are weakest element in security
- Awareness
    - Make users recognize security
    - Prerequisite to training

    - Posters, memos, courses, etc.
- Training
    - Teaching how to perform work tasks
    - Sometimes required before access to network is allowed
    - Provided in-house
- Education
    - Students learn more than what they need to know
    - For people pursuing certification or promotion
    - For personnel seeking security positions

Business Continuity Planning

- Project Scope and Planning
    - Business Organization Analysis
        - Who are the stakeholders to BCP planning?
            - Senior management
            - Operational departments
            - Critical support services
    - BCP Team Selection
        - Departmental representatives
        - Legal representatives
        - IT and Security representatives
        - Senior management
    - Approval of Senior Management
        - Explain benefits of BCP
            - Cost of disaster
            - Regulatory requirements
            - Legal consequences
            - Loss of customer trust
    - Resource Requirements
        - BCP Development
            - Manpower
        - BCP Testing, Training, and Maintenance
            - Manpower and some material costs
        - BCP Implementation
            - Manpower and large material costs
- Business Impact Assessment
    - Determine Recovery Goals
    - Approaches
        - Quantitative

    - Qualitative
  - Steps
    - Identify Priorities
      - Critical Processes
        - Maximum Tolerable Downtime
        - Recovery Time Objective
    - Risk Analysis
      - Risk Identification
      - Likelihood Assessment
      - Impact Assessment
    - Resource Prioritization
- Continuity Planning
  - Minimize impact of risks
  - Steps
    - Strategy Development
      - Know risks which require mitigation
      - Know resources to be allocated
    - Provisions and Processes
      - Risk mitigation mechanisms
      - Categories
        - People
          - Most valuable asset
          - Takes priority over everything else
          - Must be provided equipment
          - Food and shelter if must stay for extended time
        - Facilities
          - Hardening
          - Alternate Site
        - Infrastructure
          - Hardening
          - Alternate Systems
    - Plan Approval
      - Senior management must approve
      - Approval gives BCP authority and weight
    - Plan Implementation
      - Schedule implementation
      - Utilize resources to achieve goals
    - Training and Education
      - Education about the plan
      - BCP Team
        - BCP Task Training

  - BCP Backup
    - BCP Task Training
  - Everyone Else
    - Plan Overview
- BCP Documentation
  - Goals
    - Provide reference if BCP members are absent
    - Track BCP history
    - Allows review of BCP plan
  - Contains
    - Continuity Planning Goals
      - Continue business in an emergency
      - MTD and RTO goals
    - Statement of Importance
      - Says why BCP plan is important
      - Signed by senior management
    - Statement of Priorities
      - List of critical activities
      - Arranged from most critical to least critical
    - Statement of Organizational Responsibility
      - "Business continuity is everyone's responsibility"
      - Expectation from employees to help in continuity
    - Statement of Urgency and Timing
      - Expresses criticality of BCP
      - Timetable of implementation
    - Risk Assessment
      - Documented results of risk assessment
      - AV, EF, ARO, SLE, ALE
    - Risk Actions (Acceptance/Mitigation)
      - Reason for risk acceptance
      - Provisions for mitigated risks
  - Vital Records Program
    - Vital Records
      - Critical business records
      - Records that need to be present when rebuilding the business
      - Identify, find, and secure vital records
  - Emergency Response Guidelines
    - Immediate response procedures
    - Individuals that should be notified
    - Secondary response procedures until BCP team arrives

        - Maintenance
            - Revise and improve the plan
            - Do not disband BCP team
            - Keep track of changes
            - Add to job descriptions
        - Testing and Exercises
            - Perform exercises to test BCP process

Laws Regulations and Compliance

- Categories
    - Criminal Law
        - To keep peace and order
        - Punishes acts against society
        - Prosecuted by federal and state governments
    - Civil Law
        - To settle matters between entities
        - Enforcement of contracts
        - Not prosecuted unless a party sues another
    - Administrative Law
        - Regulation of government agencies
        - Granted to executive branch
        - Must comply with civil and criminal law
    - Religious Law
- Laws
    - Comprehensive Crime Control Act 1984 (CCCA)
        - Coverage
            - Federal computers
            - Offending interstate computers
        - Provisions
            - Unauthorized access to systems or information
            - Fraud using federal systems
            - Damaging federal systems exceeding $1000
            - Modify medical records impairing medical care of individual
            - Trafficking passwords affecting interstate commerce
    - Computer Fraud and Abuse Act 1986 (CFAA)
        - Amends CCCA 1984
        - Coverage
            - CCCA 1984
            - Federal interest computers

      - Government computers
      - Financial institution computers
  - Provisions
    - Same as CCCA 1984
- Computer Fraud and Abuse Act 1994 (CFAA)
  - Amends CFAA 1986
  - Coverage
    - CFAA 1986
    - Interstate commerce computers
  - Provisions
    - Same as CFAA 1986
    - Creation of malware
    - Imprisonment of offenders
    - Authority for victims to sue
- Computer Security Act of 1987 (CSA)
  - Federal system security baselines
  - Provisions
    - Gives NIST authority to develop standards
      - For non-classified federal systems
      - NIST still gets advice from NSA
      - NSA retains authority for classified systems
    - Enacts said standards and guidelines
    - Security plans must be established
    - Mandatory periodic training
- Federal Sentencing Guidelines 1991 (FSG)
  - Punishment guidelines for computer crime
  - Provisions
    - Requires due care from executives
    - Due diligence reduces punishment
    - Burdens of proof for negligence
      - Accused must have legal obligation
      - Accused failed to comply to standards
      - Causal relationship between negligence and damages
- National Information Infrastructure Protection Act of 1996 (NIIPA)
  - Extends CFAA 1994 to include infrastructure systems
  - Coverage
    - CFAA 1994
    - National infrastructure computing systems
- Paperwork Reduction Act of 1995 (PRA)
  - Request for information from public requires OMB approval

        - OMB: Office of Management and Budget
        - Includes
            - Forms
            - Interviews
            - Record-keeping requirements
- Government Information Security Reform Act of 2000 (GISRA)
    - Amends PRA 1995
    - Required government agencies to implement an InfoSec programs
    - Created "mission-critical system" category
        - A national security system
        - Protected by classified information procedures
        - Breach would result in debilitating impact of an agency
    - Agency leaders responsible for information system security
- Federal Information Security Management Act 2002 (FISMA)
    - Replaces GISRA
    - Required government agencies to implement an InfoSec programs
    - Include activities of contractors in security management programs
    - NIST is responsible for FISMA guidelines
    - Requirements
        - Periodic risk assessment
        - Policies and procedures based on risk assessment
        - Security Awareness Trainings
        - Testing of Policies and Procedures
        - Remediation plans
        - Incident response plan
        - Continuity of operations plan
- Digital Millennium Copyright Act (DMCA)
    - Prohibits attempts to circumvent copyright protection mechanisms
    - Limits liability of ISPs for transitory activities
        - Transmission initiated by person other than provider
        - Transmission must be automated without selection of material by ISP
        - ISP does not determine recipient
        - Intermediate copies not accessible to anyone and not retained
        - Material transmitted without modification to content
    - Service providers must respond promptly to remove copyrighted materials
    - Allows backup of backup copies of software
        - Must be deleted when no longer needed
    - Applies copyright law to content published on internet
- Economic Espionage Act of 1996

  - Protects U.S. trade secrets
  - Stealing trade secrets to benefit foreign agent
    - $500,000 fine
    - 15 years in prison
  - Stealing trade secrets in general
    - $250,000 fine
    - 10 years in prison
- Uniform Computer Information Transactions Act (UCITA)
  - Regulates computer business transactions
  - Addresses software licensing
  - Backs validity of shrink-wrap and click-wrap licensing
  - Allows users to reject agreements and get refunds
- Fourth Amendment
  - Prevents unreasonable searches and seizures of houses
  - Requires probable cause before search is conducted
- Privacy Act of 1974 (PA)
  - Agencies must have consent of person before disclosing their info to others
  - Agencies must only maintain necessary records
  - Agencies must destroy records no longer needed
- Electronic Communication Privacy Act 1986 (ECPA)
  - Protects electronic privacy of individuals
  - Prohibits interception of electronic communications
  - Prohibits unauthorized disclosure of communications
- Communications Assistance for Law Enforcement Act 1994 (CALEA)
  - Requires all carriers to make wiretaps possible for law enforcement
  - Requires a court order
- Economic Protection of Proprietary Information Act of 1996 (EPPIA)
  - Extends definition of property to include proprietary economic information
  - Theft no longer restricted by physical constraints
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Governs health insurance and health maintenance organizations
  - Privacy and security regulations for organizations storing patient information
  - Defines the rights of individuals subject to medical records
- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
  - Updates HIPAA's privacy and security requirements
  - Business associates of organizations under the scope of HIPAA must comply with it as well
  - Requires business associate agreement
  - Added data breach notification requirement

- SB 1386
  - California law requiring disclosure of breach to affected individuals
  - Breach includes disclosure of unencrypted copies of:
    - SSN
    - Driver's License Number
    - State Identification Card Number
    - Credit or Debit Card Number
    - Bank Account Number + Security Code
    - Medical Records
    - Health Insurance Information
- Children's Online Privacy Protection Act of 1998 (COPPA)
  - Applies to websites that caters to children
  - Requires privacy notice
    - States type of collected information
    - Which information is disclosed to 3rd parties
  - Parents must be able to review and delete children's information
  - Parental consent required for info collection on children younger than 13
- Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Relaxed restrictions on information sharing between financial organizations
  - Still provides limitations on what sort of information could be exchanged
  - Institutions required to provide privacy notice to all customers
- USA PATRIOT Act of 2001
  - Expanded power of law enforcement to monitor electronic communications
  - Police can now obtain blanket wiretapping warrants
  - ISPs can voluntarily provider government with detailed information
  - Government can obtain detailed information on user activity with a subpoena
  - Amends CFAA and adds more severe penalties
- Family Educational Rights and Privacy Act (FERPA)
  - For educational institutions receiving funding from government
  - Parents and students given right to inspect educational records
  - Parents and students given right to request correction of records
  - Schools may not release personal information from student records without written consent
- Identity Theft and Assumption Deterrence Act of 1998
  - Before: defrauded creditors were the only victims of identity theft
  - Now: the person with stolen identity is also the victim
  - Provides severe penalties of 15 years and $250,000
- European Union Privacy Law of 1995
  - Requires that personal data processing meet one of the following criteria
    - Consent

            - Contract
            - Legal obligation
            - Vital interest of the data subject
            - Balance between interest of data holder and subject
        - Outlines rights of data subjects
            - Right to access data
            - Right to know data source
            - Right to correct inaccurate data
            - Right to not consent to data processing
            - Right of legal action if rights are violated
        - Organizations that want to operate in the EU must comply to these
        - Department of Commerce certifies "safe harbor" businesses
        - Requirements for "safe harbor"
            - Notice
                - Subjects must know which info is collected from them
            - Choice
                - Opt-out policy required for data shared with 3rd parties
                - Opt-in policy required for sensitive information
            - Onward Transfer
                - Data can only be shared with other safe harbor organizations
            - Access
                - Data subjects must be able to access the data stored about them
            - Security
                - Data must be secure from loss, misuse, and disclosure
            - Data Integrity
                - Reliability of data must be maintained
            - Enforcement
                - Dispute process must be available to subjects
    - Sarbanes-Oxley Act Of 2002
        - Protect investors from fraudulent accounting activities by corporations
- Intellectual Property
    - Copyright
        - Original works of authorship
        - For art and software
        - Protects expression rather than idea
        - Automatically granted to creator
        - Can be work for hire as well
        - Protected until 70 years after death of last author
        - Protected until 95 years of publication for anonymous works

        - Indicated by (c) symbol
    - Trademark
        - Brand name, logos, slogans, etc.
        - Avoids confusion in marketplace
        - Does not have to be registered
        - Indicated by TM symbol if not registered
        - Can also be registered
        - Indicated by (R) symbol if registered
        - Renewed for unlimited successive 10-year periods
        - Requirements
            - Must not be similar to another trademark
            - Must not describe the product
    - Patent
        - For inventions, hardware, and manufacturing processes
        - Not all software can be patented
        - Protects expressions rather than idea
        - Requirements
            - Inventions must be new and original
            - Must be useful and must actually work
            - Must not be obvious (e.g. collection rainwater with a cup)
    - Trade Secret
        - Business-critical intellectual property
        - Not disclosed to competitors or anyone
        - Applying for copyright or patent would require disclosure
        - Anyone who has access to it needs a Non-Disclosure Agreement
- Licensing
    - Contractual License
        - Written contract
        - Signing = acceptance
        - Active consent
    - Shrink-wrap License
        - Written on software packaging
        - Braking package = acceptance
        - No active consent
    - Click-through License
        - Written on software box or documentation
        - Clicking "I Agree" = acceptance
        - Active consent
    - Cloud Service License
        - Agreement flashed on the screen

        - Clicking "I Agree" = acceptance
        - Active consent
- Import/Export
    - Computer Export Controls
        - No high-performance computing exports to countries:
            - Posing a threat to nuclear proliferation
            - Sponsoring terrorism
            - Includes
                - India
                - Pakistan
                - Afghanistan
                - Cuba
                - North Korea
                - Sudan
                - Syria
    - Encryption Export Controls
        - Export used to be banned
        - Export now possible
        - Requires Commerce Department review
- Privacy
    - Right to privacy not in constitution
    - Still upheld by numerous courts
    - U.S. Privacy Laws
        - Fourth Amendment
        - Privacy Act of 1974
        - Electronic Communication Privacy Act 1986
        - Communications Assistance for Law Enforcement Act 1994
        - Economic Protection of Proprietary Information Act of 1996
        - Health Insurance Portability and Accountability Act 1996
        - Health Information Technology for Economic and Clinical Health Act of 2009
        - Children's Online Privacy Protection Act of 1998
        - Gramm-Leach-Bliley Act of 1999
        - USA PATRIOT Act of 2201
        - Family Educational Rights and Privacy Act
        - Identity Theft and Assumption Deterrence Act of 1998
    - Privacy in Workplace
        - There is no reasonable expectation of privacy when using employer equipment
        - Make sure there is no implied expectation of privacy in the office:
            - State it in the employment contracts

            - State it in corporate acceptable use and privacy policies
            - State it in logon banners
            - State it on warning labels in telephones and computers
- Data Breach Notification
    - Health Information Technology for Economic and Clinical Health Act of 2009
    - SB 1386
- Compliance
    - Payment Card Industry Data Security Standard (PCI DSS)
        - For entities that accept, store, and process credit cards
        - Requirements
            - Install firewall
            - Do not use default passwords
            - Protect cardholder data
            - Encrypt transmission of cardholder data
            - Protect systems against malware by updating antivirus programs
            - Develop secure systems and applications
            - Restrict access to cardholder data by business need-to-know
            - Authenticate access to system
            - Restrict physical access to cardholder data
            - Track and monitor all access to network resources and cardholder data
            - Regularly test security systems and processes
            - Maintain a policy that addresses information security for all personnel
        - Might also require external auditors to report to regulators
- Contracting and Procurement
    - Make sure to review vendor security policies
    - Questions to ask
        - Information stored, processed, and transmitted?
        - Information protection controls?
        - How information is segregated from other clients?
        - Encryption algorithms and key management?
        - Types of security audits performed?
        - Third parties used by the vendor?
        - Location of data storage, processing, and transmission?
        - Incident response process?
        - How is integrity ensured?

Asset Classification

- Sensitive Data
    - Personally Identifiable Information
        - Can be used to distinguish an individual's identity
        - Information linkable to an individual
    - Personal Health Information
        - Processed by health organizations, schools, employer
        - Relates to past, present, or future health condition of individual
        - Relates to past, present, or future payment for healthcare
    - Proprietary Data
        - Helps maintain competitive edge of organization
- Sensitive Data Management
    - Marking
        - Applying classification labels
            - Digital Labels
                - Headers and Footers
                - Watermarks
                - Metadata
                - Background Colors
            - Physical Labels
                - Hardware Color
                - Text Label
        - Label unclassified assets as well
            - Prevents omission
        - Identify downgrade procedures
            - Purging, etc.
            - Usually prohibited
            - Destruction and repurchasing is safer
    - Handling
        - Secure use and transport of data based on classification
        - Backup should be as protected as production data
        - Log, monitor, and audit to ensure compliance and accountability
    - Storage
        - Apply appropriate controls based on classification
            - Encryption
                - AES256
            - Physical Security
                - Safes
                - Secure Rooms

      - Cabinets
      - HVAC
    - Data is more valuable than the media
      - Buy high quality media
      - Buy media with built-in security
  - Destruction
    - Data disposal requirements based on classification
    - Prevents unauthorized disclosure
    - Data Remanence
      - Magnetic Media
        - Residual magnetic footprint of data on hard drive
        - Can be recovered even if data was overwritten
        - Use a degausser to remove it
      - Solid State Drives
        - No reliable way to destroy data
        - Has built-in erase commands, but ineffective
        - Physical destruction is best solution
    - Terms
      - Erasing
        - Normal delete operation
        - Frees file space but doesn't remove data
        - Data *might* be overwritten eventually
      - Clearing
        - Overwriting, essentially
          - Write a single character, its complement, and then random data
        - Bad and spare sectors are not overwritten
        - Might still be recoverable
      - Purging
        - Prepares media for less secure environments
        - Involves both clearing and degaussing
      - Declassification
        - Involves purging and changing media classification
        - Not recommended; destruction is better
        - Organization risks an undiscovered recovery technique
      - Sanitation
        - Umbrella term referring to removal of sensitive data from media
        - Can involve purging, or destruction, etc.
      - Degaussing
        - Using strong magnets to erase data on media

                - Destroys media electronics sometimes
                - Does not affect CDs, DVDs, or SSDs
            - Destruction
                - Physical destruction, basically
                - Crushing, shredding, incineration, chemicals, etc.,
                - Most secure data destruction method
    - Retention
        - Data retention requirements based on classification
        - Can reduce liabilities
        - Record Retention
            - Retaining important information as needed
            - Timeframe identified by regulation or organization policy
        - Media/Hardware Retention
            - Retaining hardware until it has to be replaced
        - Personnel Retention
            - Retaining personnel knowledge
            - Ensuring personnel don't violate NDA
- Data Classifications
    - Allows appropriate controls to be implemented for assets
    - Government
        - Focuses on value to national security
        - Classified
            - Top Secret (Class 3)
                - Disclosure = exceptionally grave damage
            - Secret (Class 2)
                - Disclosure = serious damage
            - Confidential (Class 1)
                - Disclosure = damage
        - Unclassified
            - Sensitive
            - Unclassified (Class 0)
                - Disclosure = no damage
                - Available via FOI request
    - Private
        - Focuses on value to organization
        - Proprietary (Class 3)
            - Disclosure = exceptionally grave damage
            - Keeps the organization competitive
            - Business depends on secrecy of this data
            - E.g. unreleased Sony movies, trade secrets, etc.
        - Private (Class 2)

        - Disclosure = serious damage
        - Personal information of staff, customers, and contractors
        - E.g. salary information
      - Sensitive (Class 1)
        - Disclosure = damage
        - Sensitive information that is not proprietary or private
        - E.g. company records, emails, etc.
      - Public (Class 0)
        - Disclosure = no damage
        - Meant for public consumption
        - Only integrity and availability is protected
        - E.g. brochures, websites, etc.

- Data States
  - Data at Rest
    - Stored on media
    - E.g. data stored in hard drive
    - Controls
      - Symmetric Encryption
        - AES
        - Triple DES
        - Blowfish (basis for bcrypt)
  - Data in Motion
    - Moving across a network
    - E.g. data moving across wired or wireless connection
    - Controls
      - Transport Encryption
        - HTTPS
          - Encrypts HTTP Data
        - TLS/SSL
          - SSL - Vulnerable to POODLE (do not use)
          - Encrypts data between sockets
        - IPSec
          - Encrypts data between two networks
          - Allows VPN solutions
          - Modes
            - Authentication Header
              - Provides Integrity
            - Encapsulating Security Payload
              - Provides Confidentiality
        - SSH/SCP/SFTP
          - Encrypted terminal sessions with file transfers

    - Data In Use
        - Data in temporary storage buffer while being used
        - E.g. data in RAM, registers, etc.
        - Controls
            - Purging after use
- Data Roles
    - Data Owner
        - Ultimately responsible for the data
        - Liable for negligence
        - Identifies data classification
        - Roles
            - Determine acceptable use policy
            - Determine security controls policy
            - Determine access and privilege policy
        - e.g. President, CEO, etc.
    - System Owner
        - Owns the system that processes data
        - Roles
            - Craft system security plan w/ data owner
            - Manage system security plan
            - Train users and personnel on acceptable use policy
            - Implement system security plan
        - e.g. IT department
    - Business/Mission Owner
        - Owns a business process that leverages systems
        - Leverages on systems to provide value to organization
        - Goals may sometimes conflict with system owners
        - e.g. Sales department
    - Data Processor
        - Processes data for a data controller (business/mission owner?)
        - Must not use data for anything else aside from intended purpose
        - e.g. 3rd party payroll processor
    - Administrator
        - Grants access to personnel
        - Follows principle of least privilege
        - Uses role-based access control model
        - Adds and removes users from roles
    - Data Custodian
        - Implements data security controls
        - Implements safe backup and storage of data based on policy

        - e.g. IT department
    - User
        - Accesses data to accomplish work tasks
        - e.g. employees, end users
- Protecting Privacy
    - Security Baselines
        - List of security controls
        - Image of a secure system
    - Scoping and Tailoring
        - Revising a standard/baseline to meet your requirements
        - e.g. removing WAF when you have no web application
        - e.g. not complying with safe harbor if you don't do business in EU
    - Selecting Standards
        - Determine which regulations apply to your service
        - e.g. PCI DSS, HIPAA, Safe Harbor

Cryptography

- History
    - Caesar Cipher
        - Used by Julius Caesar
        - ROT 3
        - Defeated by frequency analysis
    - Engigma
        - Used by Germans
        - Defeated by project Ultra
    - Purple Machine
        - Used by Japanese
- Goals
    - Confidentiality
        - Date at Rest
        - Data in Motion
    - Integrity
    - Authentication
    - Non-repudiation
- Concepts
    - Kerchoff Principle
        - Cryptosystem must be secure even if mechanism disclosed
        - Key is the only thing that needs to be a secret
        - Security by design instead of obscurity

  - Cryptography
    - Methods to keep information secret
  - Cryptanalysis
    - Art of defeating cryptography
  - Cryptology
    - Cryptography + Cryptanalysis
  - Codes
    - Representation of words or messages
    - e.g. 10-4 = "Acknowledged"
    - Not always meant to provide confidentiality
  - Ciphers
    - Hides true meaning of messages
    - Always meant to provide confidentiality
  - Confusion
    - Disassociation of relationship between plain text and key
  - Diffusion
    - Slight change in plain text changes the whole cipher text
  - Frequency Analysis
    - Examination of recurring data
    - E.g. some letters of the alphabet occur more than the others
  - Period Analysis
    - Frequency examination based on repeated use of key
  - Block Ciphers
    - Encryption occurs per chunk
  - Stream Ciphers
    - Encryption occurs per bit or byte
- Mathematics
  - Boolean Mathematics
    - AND
    - OR
    - NOT
    - XOR
  - One-way Functions
    - Producing output is easy
    - Deriving input is hard
    - E.g. factoring very large numbers
  - Nonce
    - Initialization Vector
    - Adds randomness to encryption process
  - Zero Knowledge Proof
    - Proving knowledge of fact without revealing fact itself

        - E.g. providing password hash instead of password
        - E.g. answering to an authentication challenge
    - Split Knowledge
        - Key Escrow
            - Parts of key sent to different escrow providers
        - M of N Control
            - M of N individuals must be present to perform high security task
    - Work Function
        - Amount of work to brute force an encryption system
        - Key length is primary factor to determining work function
- Ciphers
    - Transposition Ciphers
        - Rearrangement of data/characters
        - Example: Columnar Transposition
            - Message is split into `len(key)` blocks/rows
            - Each letter of the key is associated with a column
            - Columns are arranged based on the value of the key letter associated with them
            - Columns are converted into strings and concatenated
    - Substitution Ciphers
        - Replacement of data/characters (ROT3)
        - Example: Vignere Cipher
            - Have a matrix of the alphabet where the letters of each row is increment by 1
            - Have columns and rows in total
            - Ci = Matrix[Ki][Pi]
    - One-Time Pads
        - Key as large as message itself
        - Each message letter is padded by each key letter
        - Unbreakable encryption scheme
        - Requirements
            - Key must be random
            - Protection of key from disclosure
            - Keys must only be used once
            - Key must be as long as message
    - Running Key Ciphers
        - AKA book cipher
        - One-time pad, except you get the key from a book
        - E.g. using a specific chapter and paragraph of Moby Dick

Modern Cryptography

- Symmetric Key Algorithms
    - Single shared key is used to encrypt and decrypt
    - AKA private key cryptography
    - Provides
        - Confidentiality
    - Advantages
        - Very fast
            - 1000 times faster than asymmetric cryptography
    - Disadvantages
        - Key distribution is hard
            - A secure channel must be established first before key is communicated
        - No non-repudiation mechanism
            - No way to prove an encrypted message came from someone since many people know the key
        - Not scalable
            - Each two-party communication in a large group requires a unique key
        - Frequent key regeneration
            - When someone leaves the group, key needs to be regenerated
- Asymmetric Key Algorithms
    - Private and public key decrypt message encrypted with the other
    - AKA public key algorithms
    - Private key must be kept private by a user
    - Public key must be known by everyone
    - Provides
        - Confidentiality
        - Integrity
        - Authentication
        - Non-repudiation
    - Advantages
        - Key distribution is simple
            - No secure channel required to start communication
        - Supports Non-repudiation mechanism
            - Since only the person knows their private key
            - Allows digital signatures to be generated
                - Hash of a message encrypted with a private key
                - Verification involves decryption using public key and cross-checking hashes
        - Scalable

      - No new key needs to be generated for each pair of communicating parties
      - New users only require generation one key pair
    - Infrequent key regeneration
      - Required only if private key is compromised
      - Key can easily be invalidated when user leaves system
  - Disadvantages
    - Very slow
      - 1000 times slower than symmetric cryptography
- Hashing
  - Production of message digest
  - One-way function
  - Summary of message's content

Symmetric Cryptography

- Key Management
  - Creation and Distribution
    - Offline Distribution
      - Sheet of paper or storage media is physically transported
      - Interception might occur via mail
      - Telephones can be wiretapped
      - Papers might get thrown in the trash
    - Public Key Cryptography
      - Requires public key infrastructure
    - Diffie-Hellman
      - No public key infrastructure is required
      - Steps
        - Parties agree on two large prime numbers
          - p and g
          - 1 < g < p
        - Each party chooses a random integer and performs
          - gi mod p
        - Results are sent to each other
        - Each party multiplies their origin random integer with received number
        - They end up with same value
  - Storage and Destruction of Symmetric Keys
    - Don't store key and data in same system
    - Provide two different individuals half the key (split knowledge)

    - Key must be regenerated when someone who knows the key leaves the organization
  - Key Escrow and Recovery
    - Allows government to get copy of key upon court order
    - Fair Cryptosystems
      - Key is divided and sent to multiple third parties
      - Court provides evidence of court order to third parties in order to retrieve key
    - Escrowed Encryption Standard
      - Provides government with technological means to decrypt ciphertext
      - Uses skipjack algorithm
- Cryptographic Life Cycle
  - Computers get faster all the time
  - Encryption algorithms will eventually get obsoleted
  - Appropriate algorithm must be used depending on how long data needs to be retained
  - Algorithm Governance Controls
    - Specifying acceptable cryptographic algorithms
    - Identifying acceptable key lengths
    - Enumerating transport protocols that may be used
- Algorithms
  - Data Encryption Standard (DES)
    - Old standard required for government communications
    - Insecure and deprecated; replaced by AES
    - Key size: 56 bits (technically 64, but 8 bits is used for parity)
    - Modes
      - ECB (Electronic Code Book)
        - Each block is encrypted separately
        - Generates the same ciphertext for the same plaintext
        - Vulnerable to cryptanalysis
      - CBC (Cipher Block Chaining)
        - Plaintext block is XORed with previous ciphertext
        - Difference from CFB: Splits messages into block before encrypting
        - Requires an Initialization Vector
        - Destroys patterns
        - Allows errors to propagate
      - CFB (Cipher Feedback Mode)
        - Streaming version of CBC
        - Difference from CBC: Encrypts once a buffer is filled
        - Requires an Initialization Vector

      - Destroys patterns
      - Allows errors to propagate
    - OFB (Output Feedback Mode)
      - Plaintext is XORed with DES-encrypted seed value
      - Seed value is re-encrypted for every block
      - Requires an Initialization Vector
      - Destroys patterns
      - Errors do not propagate
    - CTR (Counter Mode)
      - Like OFB but incrementing counter is used rather than DES of previous seed value
      - Requires an Initialization Vector
      - Destroys patterns
      - Errors do not propagate
- Triple DES (3DES)
  - Three passes of DES algorithm
  - Produces a more secure encryption
  - Uses 3 or 2 keys depending on the mode
  - Variants
    - EEE3 (three keys)
      - E(K1,E(K2,E(K3,P)))
      - Total key length: 168
    - EDE3
      - E(K1,D(K2,E(K3,P)))
      - Total key length: 168
    - EEE2
      - E(K1,E(K2,E(K1,P)))
      - Total key length: 112
    - EDE2
      - E(K1,D(K2,E(K1,P)))
      - Total key length: 112
- International Data Encryption Algorithm (IDEA)
  - Patented by Swiss developers
  - Used in PGP
  - Block size: 64
  - Key size: 128 (divided into 52 16-bit keys)
  - Has same modes as DES
- Blowfish
  - Basis of bcrypt
  - Used in SSH

    - No license required
    - Faster than DES an IDEA
    - Block size: 64
    - Key size: 32-448
  - Skipjack
    - Escrowed Encryption Standard (EES)
    - Supports escrow of encryption keys
    - Not adopted by the public
    - Block size: 64
    - Key size: 80
  - Rivest Cipher 5 (RC5)
    - By Rivest, Shamir, and Adleman
    - Block size: 32, 64, 128
    - Key Sizes: 0-2048
  - Two-Fish
    - AES finalist
    - Includes pre-whitening and post-whitening
    - Prewhitening
      - Before first round of encryption
      - XORing plaintext with separate subkey
    - Postwhitening
      - After 16th round of encryption
      - XORing plaintext with separate subkey
    - Block size: 128
    - Key size: 256
  - Rijndael
    - Block sizes: 128, 192, 256
    - Key sizes: 128, 192, 256
    - Chosen as AES
  - Advanced Encryption Standard (AES)
    - Meant to replace DES
    - Rijndael with 128 block size
    - Key sizes: 128, 192, 256

Asymmetric Cryptography

- Private and Public Keys
  - Decrypts each other
  - Private Key

- Kept private
- Used to generate digital signatures
- Used to decrypt confidential messages

- Public Key
  - Published
  - Used to verify digital signatures
  - Used to encrypt confidential messages
- Algorithms
  - Rivest Shamir Adlement (RSA)
    - Key Length: 1024
    - n = p * q
    - select random e where e < n and e and (p-1)(q-1) is relatively prime
    - Find d such that (ed-1)mod(p-1)(q-1) = 1
    - e and n are public keys
    - d is private key
    - Encryption: C = Pe mod n
    - Decryption: P = Cd mod n
  - Merkle-Hellman Knapsack
    - Like RSA but relies on super-increasing sets
    - Proven ineffective in 1984
  - El Gamal
    - Based on Diffie-Hellman
    - Not patented
    - Doubles length of data it encrypts
  - Elliptic Curve
    - Key Length: 160
    - Uses elliptic curve mathematics
    - Elliptic curve definition:
      - y2 = x3 + ax + b
    - Elliptic Curve Group
      - Points that lie on the elliptic curve
      - O = located at infinity
      - Two points can be added: P + Q
      - Can be multiplied: Q = xP (Q is multiple of P)
      - It's extremely difficult to find X
    - 160-bit key is just as strong as 1024 RSA key
- Key Management
  - Use publicly-vetted encryption system
  - Select appropriate length keys

    - Ensure that private key is secret
    - Retire keys after they're no longer useful
    - Keep backups of your key

Hash Functions

- Facts
    - Converts messages into fixed length outputs
    - Generated value is called a Message Digest
    - Used to ensure message integrity
    - Used as a component of Digital Signatures
- Requirements (According to RSA)
    - Input can be any length
    - Output has fixed length
    - Easy to compute for any input
    - Is one-way
    - Collision-free
- Algorithms
    - SHA
        - Facts
            - Stands for Secure Hash Algorithm
            - Developed by NIST
            - Part of Secure Hash Standard
        - Algorithms
            - SHA-1
                - Block Size: 512
                - Output Size: 160
            - SHA-2
                - SHA-256
                    - Block Size: 512
                    - Output Size: 256
                - SHA-192
                    - Block Size: 512
                    - Output Size: 192
                    - Truncated SHA-256
                - SHA-512
                    - Block Size: 1024
                    - Output Size: 512
                - SHA-384
                    - Block Size: 1024

          - Output Size: 384
          - Truncated SHA-512
      - SHA-3
        - Keccak Algorithm
        - Not yet published
  - MD Series
    - Facts
      - Developed by Ronald Rivest
    - Algorithms
      - MD2
        - Block Size: 16
        - Output Size: 128
        - Facts
          - Proved to be reversible
      - MD4
        - Block Size: 512
        - Output Size: 128
        - Facts
          - Uses 3 rounds
          - Block data must be 64 bits less than 512
      - MD5
        - Block Size: 512
        - Output Size: 128
        - Facts
          - Uses 4 rounds
          - Block data must be 64 bits less than 512
          - Subject to collisions
        - HAVAL
          - Hash of variable length
          - MD5 variant

Digital Signatures

- Facts
  - Ensures non-repudiation
  - Message digest encrypted with a private key
  - Verified using the public key
  - Does not provide ny privacy
- Achieves
  - Non-repudiation

    - Authentication
    - Integrity
- Generation
    - Message is hashed
    - Hash is encrypted with sender private key
    - Encrypted hash is attached to the message
    - Message with signature is sent
- Verification
    - Signature is decrypted with sender public key
    - Message is hashed
    - Decrypted hash is compared to hash of message
    - If same, signature is valid
- Hashed Message Authentication Code (HMAC)
    - Facts
        - Just like Digital Signatures, but uses a symmetric algorithm
        - Provides no non-repudiation
        - Operates more efficiently
- Digital Signature Standard
    - Acceptable Digital Signature Algorithms
        - Digital Signature Algorithm (DSA)
        - Rivest, Shamir, Adleman (RSA)
        - Elliptic Curve DSA (ECDSA)
    - Acceptable Hashing Algorithms
        - SHA-2

Public Key Infrastructure

- Allows communications between previously unknown parties
- Components
    - Certificates
        - Endorsed copies of public key
        - E.g. Public key digitally signed by Certificate Authority
        - Information Contained (X.509 Certificate)
            - X.509 Version
            - Serial Number
            - Signature Algorithm Identifier
            - Issuer Name
            - Validity Period
            - Subject's Name

        - Subject's Public Key
    - Used to establish SSL connections
  - Certificate Authorities
    - Notarizes digital certificates
    - People trust them and they trust various organizations
    - You prove your identity to CA and they vouch for you
    - Examples
      - Symantec
      - Thawte
      - GeoTrust
      - GoDaddy
      - Comodo Limited
      - DigiCert
      - etc.
    - Default trusted CAs are built-into the browser
  - Registration Authorities
    - Assist CA with verifying user identities
- Certificate Path Validation
  - Verification of the chain of trust from the root down to the client
- Certificate Generation and Destruction
  - Enrollment
    - Registration to a Certificate Authority
    - Steps
      - Providing documents / physically appearing, etc.
      - User provides CA with public key
      - CA creates X.509 digital certificate
      - CA digital signs the certificate
      - CA provides user signed copy of certificate
  - Verification
    - Steps
      - Verify digital signature of certificate
      - Verify that the CA is trusted
      - Check if the certificate is not in a CRL
      - Check if certificate contains data that us trusted (e.g. email/domain)
  - Revocation
    - Reasons
      - Compromise of private key
      - Incorrectly issued certificate
      - Certificate details changed
      - Security association changed (e.g. subject no longer employed)

    - Verification
        - Certificate Revocation List (CRL)
            - List of revoked certificate serial numbers
            - Has to be downloaded and cross-checked
            - May have some latency issues
        - Online Certificate Status Protocol (OCSP)
            - Allows lookup of certificate status without downloading CRL
            - Allows real-time verification
            - Return status
                - Valid
                - Invalid
                - Unknown

Applied Cryptography

- Portable Devices
    - Disk/Volume Encryption
    - Trusted Platform Modules
- Email
    - Pretty Good Privacy
        - By Phil Zimmerman
        - Uses web of trust
            - Decide which users to trust
            - Transitive trust takes effect
        - Commercial Version
            - Key Exchange: RSA
            - Encryption: IDEA
            - Message Digest: MD5
        - Freeware Version
            - Key Exchange: Diffie-Hellman
            - Encryption: CAST
            - Message Digest: SHA-1
    - S/MIME
        - De facto standard for encrypted email
        - Key Exchange: X.509 Certificates
        - Public Key Protocol: RSA
        - Symmetric Encryption: AES and 3DES
        - Supported by desktop mail clients
        - Not supported by web clients
- Web Applications

    - SSL/TLS/HTTPS
        - Originally by Netscape, adopted by Microsoft
        - Steps
            - Browser retrieves website certificate
            - Browser extracts public key from certificate
            - Browser generates random symmetric key
            - Public key is used to encrypt random symmetric key
            - Encrypted key is sent to webserver
            - Server decrypts symmetric key using its private key
            - All future messages are encrypted using the symmetric key
        - POODLE Attack
            - Makes TLS fallback to SSL 3.0
            - Organizations now just drop support for SSL
- Steganography and Watermarking
    - Embedding secret messages within other files
    - May be used to add digital watermarks to assets
    - Can be used to protect intellectual property
    - Watermark can be traced back to original copy
- Digital Rights Management
    - Music
    - Movie
        - Content Scrambling System
            - Enforces playback and region restrictions on DVDs
            - Broken with release of DeCSS tool
        - Advanced Access Content System (AACS)
            - Protects content stored on Blu-Ray and HD DVD
            - AACS encryption keys have been retrieved and posted online
    - E-Book
        - Most successful type of DRM
            - Adobe Digital Experience Protection
                - DRM for e-books
                - Encrypted with AES
                - RSA to protect AES key
                - Used by a variety of e-readers
    - Video Game
        - Make video games dependent on internet to verify the game license
    - Document
        - Prevents actions from being performed on a document
        - Examples
            - Reading a file

      - Modifying a file
      - Removing watermarks
      - Downloading/saving
      - Printing
      - Taking screenshots
- Networking
  - Circuit Encryption
    - Link Encryption
      - Encrypts communication between two network locations
      - Entire packets are encrypted
      - Slower but less susceptible to sniffing
      - Done beneath transport layer
      - E.g. two office networks
    - End-to-end Encryption
      - Encrypts communication between two hosts
      - Only data is encrypted
      - Faster but more susceptible to sniffing
      - Done in transport layer or above
      - E.g. client and webserver
  - IPSec
    - IETF standard for setting up secure comms channel
    - Parties can be two gateways, two systems, etc.
    - Uses public key cryptography
    - Modes
      - Transport Mode
        - Between two gateways
        - Uses L2TP (layer 2 tunneling protocol)
      - Tunnel Mode
        - Between two hosts (peer-to-peer)
    - Components
      - Authentication Header
        - Uses public keys(?)
        - Authentication
        - Access Control
        - Integrity
        - Non-repudiation
        - Prevents replay attacks
      - Encapsulating Security Payload
        - Uses symmetric keys(?)
        - Encryption

        - Some authentication
        - Prevents replay attacks
        - Sometimes used without AH
    - Security Association
      - Represents communication session
      - Records configuration status about connection
      - Represents a one-way connection
      - Additional SA must be setup per direction and IPSec component
    - Internet Security Association Key Management Protocol (ISAKMP)
      - Establishes, modifies, and deletes Security Associations
      - Requirements for ISAKMP
        - Authenticate communicating peers
        - Create and management security associations
        - Provide key generation mechanisms
        - Protect against threats (DOS, replay attacks, etc.)
  - Wireless Networking
    - Wired Equivalent Privacy
      - Not secure - do not use
      - 64 and 128-bit encryption
    - Wi-Fi Protected Access
      - WPA
        - Adds TKIP to the mix
        - Temporal Key Integrity Protocol
        - Secure IV generation
      - WPA2
        - Uses CCMP instead of TKIP
        - Uses AES instead of RC4
    - 802.1X
      - For network authentication
      - Clients that connect to a network are authenticated
      - Client runs a supplicant application
      - Supplicant communicates with Authentication Server

Cryptographic Attacks

- Analytic Attack
  - Reduces complexity of the algorithm
- Implementation Attack
  - Attacks specific implementations
- Statistical Attack

    - Exploits statistical weaknesses
        - Inability to produce random numbers
        - Floating-point errors
- Brute Force
    - Trying every possible key
    - Time to break depends on length of key
    - Approaches
        - Rainbow table
            - Table of hashes and corresponding values
            - Makes brute force attacks faster
            - Prevented by salting passwords
                - Adding a random nonce before hashing a password
                - Salt is stored alongside password hash
                - Salt is added to any new string that needs to be compared w/ password
                - This increases the difficulty of brute force attacks
        - Specialized computing hardware
- Ciphertext Only / Frequency Analysis
    - Only ciphertext is available to cryptanalyst
    - One can perform a frequency analysis attack
        - E T O A I are the most frequent letters of the alphabet
            - If these letters are also the most common, expect a transposition cipher
            - If other letters are more common, expect a substitution cipher
- Known Plaintext
    - Attacker knows plaintext and corresponding ciphertext
- Chosen Plaintext Attack
    - Attack can encrypt any plaintext of his choosing
- Chosen Ciphertext
    - Attacker has ability to decrypt certain portions of ciphertext
- Meet in the Middle
    - Defeats algorithms that use two rounds of encryption
    - This is what broke 2DES
    - Process
        - Have specific plaintext
        - Encrypt it with every possible key
        - Each ciphertext is decrypted with all possible keys
        - When match is found, the pair of keys represent both portions of double encryption
    - Key strength is only 2^n rather than 2^n * 2^n
    - Only adds minimal amount of protection

- Man in the Middle
    - Interception of communications
    - Key is intercepted and replaced
    - A different secure session is started by MIT between the 2 hosts
    - 2 hosts don't know they're not communicating with each other
- Birthday Attack
    - AKA collision attack / reverse hash matching
    - Attacker replaces signed communication with another message w/c has the same hash
- Replay Attack
    - Used against algorithms w/c do not use temporal protections
    - E.g. algorithms without initialization vectors, etc.
    - Captured messages can simply be resent in order to trigger some action

Secure Design Principles

- Objects and Subjects
    - Subject
        - User/process trying to access a resource
    - Object
        - A resource a user/process wants to access
- Closed and Open Systems
    - Open System
        - System built on agreed-upon industry standards
        - Easy to integrate with other systems
        - More likely to be targeted
    - Closed System
        - Works with narrow range of other systems
        - Usually proprietary
        - Less likely to be targeted
- Open Source and Closed Source
    - Open Source
        - Source code is exposed to the public
        - Depends on public scrutiny to evaluate and secure
    - Closed Source
        - Source code is hidden from the public
        - Depends on vendor to evaluate and secure
        - Also called "commercial"
        - Can still be an open system
- Ensuring CIA

    - Confinement
        - Restricting program to a specific memory and resource space
        - Also called "sandboxing"
        - Implemented by the operating system
    - Bounds
        - The range of memory and resources that a program can operate in
        - Enforced by the operating system
        - Physical Bounding
            - Processes can be required to run on a range that is physically separated from other processes
        - Logical Bounding
            - Process can be allowed to run on a range that is in the same physical range of other processes
    - Isolation
        - The state of being confined
        - Program is prevented from accessing memory of another processes
        - OS provides resource sharing capabilities instead
- Controls
    - Control
        - Limits subject access to an object
    - Mandatory Access Control
        - Subjects and objects have static labels
        - Labels determine access right
    - Rules Based Access Control
        - Uses rules to determine access right
        - Rules grant access rights to objects
    - Discretionary Access Control
        - Subjects define access rules to objects
        - If they have the authority to, that is
- Trust and Assurance
    - Trusted System
        - One which protects data for many types of users
    - Assurance
        - Degree of confidence in satisfaction of security needs
        - Needs to be maintained
        - Changes decrease assurance, hence, reevaluation is needed

Security Models

- Concepts

    - Security Model
        - Maps abstract statements into a security policy
        - Used to measure system support of security policy
    - Tokens, Capabilities, and Labels
        - Tokens
            - Separate object associated with a resource
            - Describes resource's security attributes
        - Capabilities
            - A list of capabilities for each object
            - Not very flexible but faster
        - Labels
            - Attached to a resource and is a part of it
            - Cannot be altered
- Models
    - Trusted Computing Base
        - Set of computing components which enforces security policy
        - Foundation of most security models
        - Restrict activities of components outside the TCB
        - Concepts
            - Security Perimeter
                - Bounds between TCB and rest of system
                - Prevents insecure communications between TCB and rest of system
                - Trusted Path
                    - Used by TCB to communicate with rest of system
                    - Adheres to strict standards to prevent compromise of TCB
            - Reference Monitor
                - Validates access to every resource
                - Grants access to resources
                - Stands between subject and object
                - Just a theory, not an actual thing
            - Security Kernel
                - TCB components that implement the reference monitor
                - Launches components that enforce reference monitor
                - Uses trusted paths to communicate with subjects
                - Mediates all resource access
    - State Machine Model
        - Describes a system that is always secure
        - All valid states are secure
        - All valid state transitions are secure

  - Also called Secure State Machine
  - Basis for other security models
  - Based on Finite State Machine
- Information Flow Model
  - Only valid information flows may be allowed
  - Prevents insecure information flows
  - Addresses covert channels
  - Focuses on flow of information
  - Composition Theories
    - Describes information flow between systems
    - Theories
      - Cascading
        - Input of one system comes from output of another
        - Example: Web server with database backend
        - A -> B -> C : Chaining
      - Feedback
        - System receives input and responds with output
        - Example: HTTP Request and Response
        - A -> B : Request
        - A <- B : Response
      - Hookup
        - System sends input to one system and sends copy to another
        - Example: CC and BCC in email
        - A -> B : To Destination
        - A -> C : To Hookup
  - Based on State Machine Model
- Noninterference Model
  - High privileged actions should not affect lower privileged subjects
  - Unauthorized parties should not be affected by information flows
  - Prevents inference attacks and covert channels
  - Based on the Information Flow Model
- Take-Grant Model
  - Describes how rights can be passed/taken from subject to subject/objects
  - Allows you to track where rights can change
  - Allows you to track where leakage can occur
  - Rules
    - Take Rule
      - Allows subjects to take rights over an object
    - Grant Rule

      - Allows a subject to grant rights over an object
    - Create Rule
      - Allows a subject to create new rights
    - Remove Rule
      - Allows a subject to remove rights it has
- Access Control Matrix
  - A matrix of subjects an objects
  - Indicates the rights each subject has over each object
  - Parts
    - Row
      - Subjects
      - Capabilities List
        - Each row shows capability of each subject
        - List of rights a subject has for every object
    - Columns
      - Objects
      - Access Control Lists
        - Each column shows subjects that have rights to object
        - List of subject that has rights to an object
    - Cells
      - Access Rights
        - Access rights of a subject to an object
- Lattice-Based Access Control
  - Subject are assigned position in a lattice
  - Positions fall between security labels
  - Subjects only access objects that are within "range"
  - Example
    - A subject between Private and Sensitive
    - Can only access an object within those two labels
- Bell-LaPadula Model
  - Prevents information flow to lower sensitivity levels
  - Protects Confidentiality
  - Does not address integrity or availability
  - Used by military organizations
  - Properties
    - Simple Security Property
      - No Read Up
      - Subjects can't read objects with higher sensitivity labels
    - (*) Security Property
      - No Write Down
      - Subjects can't write to objects with lower sensitivity labels

      - Unless performing declassification, which is a valid operation
    - Discretionary Security Property
      - An access matrix is used to enforce discretionary access control
  - Trusted Subject
    - Exception to * Security Property
    - Can declassify objects
  - Based on State Machine and Information Flow Model
- Biba Model
  - Prevents information flow to higher integrity levels
  - Protects Integrity
  - Prevent unauthorized modification of objects
  - Protects object consistency
  - Does not address confidentiality or availability
  - Used by commercial organizations
  - Properties
    - Simple Integrity Property
      - No Read Down
      - Subjects can't read objects at lower integrity levels
    - (*) Integrity Property
      - No Write Up
      - Subjects can't write objects at higher integrity levels
  - Based on Bell-LaPadula Model
  - Based on State Machine and Information Flow Model
- Clark-Wilson Model
  - Access to subject must be mediated through a program
  - Program enforces well-formed transactions
  - Protects
    - Confidentiality
    - Integrity
  - Constrained Interface
    - Enforces well-formed transactions
    - Enforces separation of duties
    - Authorizes transactions
  - Access Control Triple
    - Subject
    - Object
    - Program/Transaction/Interface
  - Constrained Data Item
    - Data items protected by the model

    - Can only be modified by transformation procedures
  - Unconstrained Data Item
    - Data not controlled by the model
    - Input and output data
  - Integrity Verification Procedure
    - Determines integrity of data items
  - Transformation Procedures
    - Used to modify a constrained data item
    - The only thing that can
    - Essentially the backbone of the model
    - Example: Store Procedure in Database
  - Restricted Interface Model
    - Provides subjects authorized information and functions
    - Subjects at different levels see different set of data
    - Like a webapp that shows you only the info and features you can access
    - Enforces separation of duties in effect
- Brewer and Nash Model / Chinese Wall
  - Focused on confidentiality
  - Uses security domains / conflict classes
  - Prevents conflict of interests
  - Based on a user's previous actions
  - Security domains are not predetermined
  - Examples
    - Separate conflict classes for accessing data of two competing companies
    - Preventing access to data irrelevant to a current operation
- Goguen-Meseguer Model
  - Focused on integrity
  - Basis for non-interference model
  - Security domains are predetermined
    - List of objects a subject can access is predetermined
    - List of operations a subject can perform is predetermined as well
- Sutherland Model
  - Focused on integrity
  - A non-interference model
  - A state machine model
  - Defines a set of system states, and transitions
  - Integrity is maintained if the defined states and transitions are used
- Graham-Denning Model

- Focused on secure creation and deletion of objects
- Specifies how to securely:
    - Create
        - Object
        - Subject
    - Delete
        - Object
        - Subject
    - Provide Right
        - Read
        - Grant
        - Delete
        - Transfer

Systems Security Evaluation Models

- Evaluation Steps
    - Certification
        - Notes
            - Initiated by a vendor
            - Test system security capabilities
            - Compare design, security criteria, and actual capabilities
            - Auditors decided if security criteria is met
            - Security criteria is based on intended use (commercial, health, etc)
            - Usually performed by a 3rd party
        - Steps
            - Choose security criteria (TCSEC/ITSEC/CC)
            - Analyze each system component based on criteria
            - Evaluate deployment environment
            - Determine level of security
    - Accreditation
        - Recognition of the certification
        - Performed by an adopting organization/customer
    - Maintenance
        - Ensuring that the security criteria is up to date
        - Ensuring that the system still meets security criteria
- Rainbow Series
    - Orange - Trusted Computer System Evaluation
    - Green - DoD Password Management Guidelines
    - Yellow - TCSEC in Specific Environments

  - Tan - Audit in Trusted Systems
  - Bright Blue - Trusted Product Evaluation for Vendors
  - Light Blue - PC Security Considerations
  - Neon Orange - Discretionary Access Controls
  - Aqua - Computer Security Terms
  - Red - Trusted Network Interpretation
  - Amber - Configuration Management
  - Burgundy - Design Documentation
  - Lavender - Trusted Distribution
  - Venice Blue - Computer Security Subsystem Interpretation
- Evaluation Models
  - TCSEC - Orange Book
    - Categories
      - D - Minimal Protection
        - Do not meet the requirement to belong to any other category
      - C - Discretionary Protection
        - C1 - Discretionary Protection
          - Access is controlled using users and groups
        - C2 - Controlled Access Protection
          - Meets requirements of C1
          - Strict logon procedures
          - Enforces media cleansing
      - B - Mandatory Protection
        - B1 - Labeled Security
          - Access is controlled using subject and object labels
        - B2 - Structured Protection
          - Meets requirements of B1
          - Ensures that no covert channels exists
          - Operator and administrators are separated
          - Enforces process isolation
        - B3 - Security Domains
          - Meets requirements of B2
          - Administrators are separated from other users
          - Reduce exposure to vulnerabilities
      - A - Verified Protection
        - A1 - Verified Protection
          - Meets requirements of B3
          - Each step of implementation is documented
    - Limitations
      - Doesn't control what users do with information once granted

        - Focused on confidentiality and doesn't work in commercial contexts
        - No physical, personnel, procedural provisions
        - Doesn't deal with networked systems
- TNI-TCSEC - Red Book
    - TCSEC with Networking Considered
    - Includes
        - CIA Rating
        - Communications Integrity
        - DoS protection
        - Intrusion prevention
    - Rating Level
        - None
        - C1 - Minimum
        - C2 - Fair
        - B2 - Good
    - Restrictions
        - Centralized networks
        - Single accreditation authority
- ITSEC
    - European security evaluation criteria
    - Corresponds to TCSEC categories
    - Categories
        - F0: F-D - Minimal Protection
        - F1: F-C1 - Discretionary Protection
        - F2: F-C2 - Controlled Access Protection
        - F3: F-B1 - Labeled Security
        - F4: F-B2 - Structured Access Protection
        - F5: F-B3 - Security Domains
    - Difference from TCSEC
        - Change doesn't require re-evaluation of a system
        - Also considers integrity
        - Doesn't require a TCB
- Common Criteria
    - A product evaluation model
    - Does not ensure that a system has no vulnerabilities
    - Helps buyers purchase products
    - An official ISO standard: ISO 15408
    - Goals
        - Add to buyer confidence in purchasing products

  - Eliminates duplicate evaluations
  - To make security evaluations more cost effective
  - To evaluation functionality and assurance of TOE/target of evaluation
- Elements
  - Protection Profiles
    - Specify security demands of customers
    - "What I want" from customers
  - Security Targets
    - Security claims of a vendor about their system
    - "I will provide" from a vendor
    - A target that a vendor sets for itself
    - Customers compare their requirements to this
  - Package
    - Additional security components provided by the vendor
    - Can be added and removed
- Process
  - Customer compares their protection profile to security targets of various vendors
  - Customer chooses product with closest security target based on published assurance levels
- Structure
  - Introduction and General Model
    - Explains the security evaluation process
  - Security Function Requirements
    - Specifies requirements for each function that needs evaluation
  - Security Assurance
    - Specifies how systems are designed, checked, and tested
- Categories
  - EAL1 - Functionally Tested
    - TCSEC: D
    - For non-serious threats to security
    - Requirements
      - Features are working as intended
  - EAL2 - Structurally Tested
    - TCSEC: C1
    - For low to moderate assurance requirements
    - Requirements
      - EAL1 is passed
      - Design information is evaluated
  - EAL3 - Methodically Tested and Checked

        - TCSEC: C2
        - For moderate assurance requirements
        - Requirements
          - EAL2 is passed
          - Security is engineered since design stage
      - EAL4 - Methodically Designed, Reviewed, and Tested
        - TCSEC: B1
        - For moderate assurance requirements
        - Requirements
          - EAL3 is passed
          - Security and commercial best practices are followed
      - EAL5 - Semi-Formally Designed and Tested
        - TCSEC: B2
        - For high assurance requirements
        - Requirements
          - EAL4 requirements
          - Specialist security engineering techniques are followed
      - EAL6 - Semi-Formally Verified, Designed, and Tested
        - TCSEC: B3
        - For high risk situations
        - Requirements
          - EAL5 requirements
          - Specialist security engineering techniques are used at all phases of design
      - EAL7 - Formally Verified, Designed, and Tested
        - TCSEC: A1
        - For highest-risk situations
        - Requirements
          - EAL6 requirements

- Certification and Accreditation Systems
  - Standards
    - Department of Defense
      - RMF - Risk Management Framework (Current)
      - DIACAP - DoD Information Assurance Certification and Accreditation Process
      - DITSCAP - Defense Information Technology Security Certification and Accreditation Process
    - Executive Branch
      - CNSSP - Committee on National Security Systems Policy (Current)

        - NIACAP - National Information Assurance Certification and Accreditation Process
    - Phases of Current Standards
        - Definition
            - Assign personnel
            - Document mission need
            - Registration and negotiation
            - Creation of System Security Authorization Agreement
        - Verification
            - Refinement of SSAA
            - Development activities
            - Certification analysis
        - Validation
            - Further refinement of SSAA
            - Certification evaluation
            - Recommendation development
            - Accreditation decision
        - Post Accreditation
            - Maintenance of SSAA
            - System operation
            - Change management
            - Compliance validation

Capabilities of Information Systems

- Memory Protection
    - Prevents processes from interacting with memory locations not allocated to them
- Virtualization
    - Allows multiple operating systems to run on the same set of hardware
- Hardware Security Module
    - Hardware cryptoprocessors
    - Used to store keys
    - Used by banks and authorities to store certificates
- Trusted Platform Module
    - Specs for a cryptoprocessor chip
    - A type of a hardware security module (HSM)
    - Provides
        - Key storage
        - Hardware encryption
            - Hard drive encryption

                - More secure
                - Key is stored in TPM so TPM is required to decrypt the hard drive
                - Hard drive can't be decrypted when put in a separate system
- Interfaces
    - Provides users access to the data
    - Must be constrained based on user privileges
        - Through hiding, if permission is not granted to a user
    - Implementation of Clark-Wilson model
- Fault Tolerance
    - Ability of a system to continue to operate when experiencing a fault
    - Achieved by adding redundant components
    - Essential element of security design

Security Vulnerabilities

- Hardware
    - Processor
        - Execution Types
            - Multitasking
                - Single processor, multiple tasks
            - Multiprocessing
                - Multiple processors, multiple tasks
                - Types
                    - SMP - Symmetric Multiprocessing
                        - Single OS distributes task to processors
                        - Multiple processors treated equally
                        - Good for simple operations
                    - MMP - Massive Multiprocessing
                        - Multiple OS environment
                        - Tasks assigned to coordinating processors
                        - Coordinating processors assign tasks to other processors
                        - Good for complex operations
            - Multiprogramming
                - Single processor, one task at a time
                - Switch to different task when one waits
                - Needs to be specially written
            - Multithreading
                - Multiple tasks in a single process

- Processing Types
    - Single State
        - Processors handle only one security level
        - The system only handles one security level
        - Access is controlled via policy
        - Cheaper
    - Multistate
        - Processors handle multiple security levels
        - The system handles multiple security levels
        - Access is controlled via technical protection mechanisms
        - More expensive
- Protection Mechanisms
    - Protection Rings
        - Lower rings, higher privilege
        - Multics has six rings, modern OSes has 4 rings
        - Rings
            - Ring 0 - Kernel
            - Ring 1 - OS Components
            - Ring 2 - Drivers
            - Ring 3 - User Programs
        - Mediated Access Model
            - Process communicate to lower ring via interfaces
        - System Call
            - Request to resources on lower level ring
            - Usually a programming interface
            - Lower ring must authorize requester
    - Process States / Operational States
        - Ready
            - Process is ready to be given a time slice
            - Initial state of a process
            - Transitions to Running State
        - Waiting / Blocking
            - Process is waiting on a resource
            - Transitions to Running State
        - Running
            - Process is currently in execution
            - Ends upon termination or end of time slice
            - Also called Problem State as errors can occur
            - Transitions to Ready, Waiting, or Stopped State

    - Supervisory
      - Process is performing privileged operation
      - States other than this is user mode
    - Stopped
      - Process is finished or must be terminated
  - Security Modes
    - Requirements
      - MAC Environment
      - Physical control of system and room
    - Modes
      - Dedicated Mode
        - Right to know everything in system
        - Permission to access everything in the system
        - Need to know everything in system
      - System High Mode
        - Right to know everything in system
        - Permission to access everything in the system
        - Need to know some things in the system
      - Compartmented Mode
        - Right to know everything in the system
        - Permission to access some things in the system
        - Need to know things to be accessed in the system
      - Multilevel Mode
        - Right to know some things in the system
        - Permission to access some things in the system
        - Need to know things to be accessed in the system
- Operating (System) Modes
  - User Mode / Problem State
    - Ring 3
    - When user applications are being executed
    - Prevents accidental damage to system
    - User programs are executed in a sandbox
      - Also called a Virtual Machine
  - Kernel Mode / Privileged Mode / System Mode
    - Ring 0 to 2

- Allows OS to perform full range of CPU instructions

- Memory
  - ROM - Read Only Memory
    - Types
      - ROM - Read Only Memory
        - Contents are written at factory
        - Can't be modified
      - PROM - Programmable Read Only Memory
        - Unwritten ROM
        - Users can write once
        - Example: CDs
      - EPROM - Erasable Programmable Read Only Memory
        - Can be erased using chemicals or UV light
      - EEPROM - Electronically Erasable Programmable Read-Only Memory
        - Can be erased electronically
        - All contents must be erased
      - Flash Memory
        - Can be erased electronically
        - Allows erasure of individual blocks
        - Example: NAND Flash, SSDs, Flash Drives
    - Issues
      - Data retention
  - RAM - Random Access Memory
    - Types
      - Real Memory
        - Main memory
        - Made up of Dynamic RAM
      - Cache RAM
        - Attached to a processor
        - Contains RAM data that is accessed frequently
        - Levels
          - Level 1 Cache
            - Attached to processor chip
          - Level 2 Cache
            - On a separate chip
        - Peripherals also have RAM caches
        - Printers have RAM caches which can load an entire job
      - Dynamic RAM
        - Loses charge over time even if power is supplied

      - Must be refreshed by CPU
      - Made up of capacitors
      - Cheaper but slower than static RAM
    - Static RAM
      - Does not lose charge over time if power is supplied
      - Does not need to be refreshed by CPU
      - Made up of flip flops
      - More expensive but faster than dynamic RAM
  - Issues
    - Pilferable
    - Data retention
    - Cold boot attack
- Registers
  - Limited amount of onboard CPU memory
  - ALU - Arithmetic Logic Unit
    - Perform arithmetic operations
    - Can directly access registers
    - Values to process must be loaded to registers first
- Addressing
  - Register Addressing
    - Value to process is in a register
    - Register address is provided by instruction
  - Immediate Addressing
    - Value to process is in the instruction
    - Provided value is used in operation
  - Direct Addressing
    - Value to process is in memory
    - Memory address of value is provided by instruction
  - Indirect Addressing
    - Address of value to process is in memory
    - Memory address of value's address is provided by instruction
  - Base + Offset Addressing
    - Address of value to process is in a register
    - Register address and offset is provided by instruction
- Secondary memory
  - Storage devices; non-volatile
  - Example: optical disk, hard drive, etc.
  - Cheaper but slower than primary memory
- Virtual Memory / Paging
  - Used to extend main memory

    - Stores overflowing contents onto secondary memory
    - Pages from main memory are "swapped" into secondary memory
    - Non-used parts of main memory are stored in page file
    - They are restored into main memory when they need to be used
  - Storage
    - Primary and Secondary
      - Primary
        - RAM
        - Data is readily available to CPU
      - Secondary
        - SSDs, CDs, hard drives
        - Data not readily available to CPU
    - Volatile and Non-volatile
      - Volatile
        - Not designed to retain data
      - Non-volatile
        - Designed to retain data
    - Random and Sequential
      - Random
        - Any memory location can be accessed immediately
        - Faster but more expensive; for shorter term storage
        - Examples: Hard Drives, RAM, CDs, DVDs
      - Sequential
        - Data prior to desired location must be read
        - Slower but cheaper; for long term storage
        - Examples: Magnetic Tape
    - Issues
      - Data Remanence
        - Files can be recovered after deletion
        - SSD blocks may retain information even after wiping
          - Some blocks might hold a copy of data when copied to lower leveled blocks
      - Theft
        - May disclose confidential information
        - Removable media are pilferable
- IO Devices
  - Types
    - Monitors
      - Van Eck radiation
        - Electronic emanations coming from monitors
        - Can be read via TEMPEST program

      - Also called Van Eck phreaking
      - CRT are more vulnerable than LCDs
  - Printers
    - Print outs can be taken if not secured
    - Printers store data locally
  - Keyboards/Mice
    - Vulnerable to TEMPEST attacks
    - Keyboards are vulnerable to keyloggers
    - Signal interception if wireless
  - Modems
    - Uncontrolled entry points into the network
    - Can establish external connections by themselves
    - Needs a telephone line
- Structures
  - Memory-Mapped IO
    - Memory space is reserved for input and output communication with device
    - CPU reads from those memory locations to read input from device
    - CPU writes to those memory locations to write output to device
    - CPU facilitates transfer of data to and from device (synchronously)
  - IRQ - Interrupt Request
    - Specific signal lines are used for CPU and device communication
    - Signal lines are identified via IRQ number
    - IRQ numbers range from 8 to 16
    - OS assigns IRQ to devices
    - Interrupt conflict happens when two devices share the same IRQ
  - DMA - Direct Memory Access
    - Like memory-mapped IO but data transfer is done asynchronously
    - CPU not needed to facilitate data transfer between memory and device
    - Steps
      - DMQ - DMA Request
        - Device requests to access memory location
        - CPU locks target memory for device
        - Device access the memory location

            - CPU continues with other tasks
          - DACK - DMA Acknowledgement
            - Device finishes accessing memory location
            - Device tells CPU that it can now access the memory location
            - CPU accesses data on shared memory location
  - Firmware
    - Hard-coded software
    - Software stored on a ROM chip
    - Not changed frequently
    - Types
      - BIOS
        - Starts up the operating system from the disk
        - Stored on an EEPROM chip
        - Phlashing: Malicious BIOS is flashed onto the ROM
      - Device Firmware
        - Mini operating systems onboard devices
        - Stored on EEPROM chip
- Client-Based Systems
  - Applets
    - Client executes code sent by the server
    - Self-contained mini programs
    - Processing burden is shifted to client
    - Privacy advantage as data is never sent to server
    - Applets can be trojans though
    - Examples
      - Java Applets
        - By Sun Microsystems
        - Sandboxed Java programs; requires JVM
        - Can run on different operating systems
        - Widely exploited
      - ActiveX Controls
        - By Microsoft
        - Non-sandboxed VB, C, C++, and Java programs
        - Has full access to Windows operating system
        - Can run on Microsoft browsers only
        - Widely exploited; usually prohibited altogether
  - Local Caches
    - ARP Cache (Poisoning)
      - Spoofed ARP replies

        - Spoofed ARP reply is used to populate ARP table
        - ARP: translates IP to MAC address
        - Spoofing: Wrong machine associated with an IP address
        - Allows man in the middle attack
    - ARP Poisoning: Static ARP Entries
        - Malicious ARP entries manually configured in the operating system
        - Must be modified locally on the machine
        - Attack Vector: Using a trojan or social engineering attack
        - Allows man in the middle attack
- DNS Cache (Poisoning)
    - HOSTS File Poisoning
        - Malicious entries added to hosts file
        - HOSTS File: local configuration file used to translate names to IPs
        - Attack Vector: Using trojan or social engineering attack
        - Allows impersonation of intended server with malicious dummy
    - Authorized DNS Server Attacks
        - Attacking DNS records stored on authoritative DNS servers
        - Affects the entire internet and gets noticed pretty quickly
        - Allows impersonation of intended server with malicious dummy
    - Caching DNS Server Attacks
        - Attacking DNS records on cache servers
        - These are provided by ISP and companies
        - Watched by less people and can occur without notice for some time
        - Allows impersonation of intended server with malicious dummy
    - DNS Lookup Address Changing
        - Changing the DNS server used by a system to a malicious one
        - Attack Vectors: intercepting DHCP responses or local system attacks vis trojans
        - Allows impersonation of intended server with malicious dummy
    - DNS Query Spoofing
        - Intercepting DNS responses and changes substitutes it with false information
        - Allows impersonation of intended server with malicious dummy

    - Temporary Internet Files
      - Contains cached website content
      - Can be poisoned to contain malicious content (client sid scripts, etc.)
      - Malicious content is invoked when cached items are accessed
  - Other Considerations
    - Emails, Phishing, and Trojans
    - Upload and Downloads
    - System Access Control
    - User Interfaces
    - System Encryption
    - Process Isolation
    - Protection Domains
    - Data and Media Labels
    - Data Backups
    - Awareness Trainings
    - Physical Protections
    - Disaster Recovery Procedures
    - Secure Coding, Configuration, and Updates
- Server-Based Systems
  - Database
    - Aggregation
      - Combining multiple instances of data
      - Produces useful information that may be classified
      - Examples: Sum, Average, Max, Min, etc.
      - Individual records might not be classified
      - Sum/Average/Max/Min of data might be classified
      - Example: record for 1 soldier and total number of troops
    - Inference
      - Deducing classified information from available information
      - Example
        - Clerk knows total salary expenses of entire company
        - A new person gets hired
        - Total salaries increase
        - The increase in salary expenses is the salary of new person
    - Data Warehousing
      - Stores large amounts of information
      - For use with specialized analysis techniques
    - Data Dictionary
      - Stores usage and access rights of data

  - Data Mining
    - Process of analyzing data warehouses
    - Search for patterns in large data sets
    - Produces metadata
  - Metadata
    - Data about data
    - Can be representation of data
    - Can be aggregation(?)
    - Something that describes the bulk of data in the warehouse
    - Examples:
      - Security incident report
      - Sales trends report
    - May be more valuable than the bulk data
  - Data Analytics
    - Examination of bulk data to extract useful information
  - Large-Scale Parallel Data Systems
    - Performs simultaneous calculations / Multiprocessing
    - Breaking down tasks into subtasks and distributing the load
- Distributed Systems
  - Cloud Computing
    - Computing is outsourced to a service provider
    - Service is accessible via the internet
    - Types
      - SaaS - Software-as-a-Service
        - Provider manages:
          - Networking
          - Storage
          - Virtualization
          - Operating System
          - Middleware
          - Applications
        - Customer uses the application
        - Examples
          - Gmail
          - Google Docs
      - PaaS - Platform-as-a-Service
        - Provider manages:
          - Networking
          - Storage
          - Virtualization

            - Operating System
            - Middleware
          - Customer manages:
            - Applications
          - Examples:
            - Heroku
        - IaaS - Infrastructure-as-a-Service
          - Provider manages:
            - Networking
            - Storage
            - Virtualization
          - Customer manages:
            - Operating System
            - Middleware
            - Applications
          - Examples:
            - Amazon Web Services EC2
    - Grid Computing
      - Computing tasks are distributed to clients
      - Clients return result to central server
      - Similar to asymmetric multiprocessing
      - Clients are able to view the data that they are handling
      - Clients are not guaranteed to return results
      - Returned results need to be validated to ensure integrity
    - Peer-to-Peer
      - No central server
      - Clients connect directly to each other
      - Examples
        - VoIP
        - Skype
        - BitTorrent
      - Same security concerns as grid computing
- Industrial Control Systems
  - DCS - Distributed Control Systems
    - Each piece of equipment have their own control system
    - Remotely accessed and managed from a central location
    - Keyword: Central Management
  - PLC - Programmable Logic Controllers
    - Single-purpose computers
    - E.g. displaying signs, marquees, etc.

        - Keyword: Single-purpose
    - SCADA - Supervisory Control and Data Acquisition
        - Standalone device networked with each other
        - Keyword: Stand-alone; Peer-to-Peer
- Web-Based Systems
    - Security Association Markup Language
        - Used to provide web-based SSO
    - Open Web Application Security Project
- Mobile Systems
    - Operating Systems
        - Android
            - Based on Linux
            - Open Source Apache License
            - Made by Google
            - App Store: Google Play
            - Can be rooted
        - iOS
            - Made by Apple
            - Closed Source
            - App Store: Apple App Store
            - Can be jailbroken
    - Issues
        - Easy to hide
        - Can be used to steal data
        - Contains sensitive info
        - Eavesdropping
    - Device Security
        - Full Device Encryption
            - Storage and voice encryption
            - Prevents reading of data
        - Remote Wiping
            - Delete entire phone data remotely
            - Can be blocked
            - Deleted data may still be recovered
        - Lockout
            - Disable access if unlock attempts fail
            - Requires a pre-configured screen lock
            - Gets longer with every failure
        - Screen Locks
            - Prevents access to unauthorized users

  - Doesn't prevent access via network or USB
  - Triggered if phone is left idle
  - Examples: PIN, patterns, biometrics, etc.
- GPS
  - Receives GPS signals
  - Apps can record GPS locations
  - Allows tracking of movement
- Application Control
  - Limits installable applications
  - Enforces application settings
- Storage Segmentation
  - Compartmentalizes various data in storage
  - Used to separate device apps from user apps
  - Can separate company data from user data
- Asset Tracking
  - Checks in at office
  - Location tracking
  - Verifies if device is still with user
- Inventory Control
  - Using mobile device to track hardware
  - Devices can read RFID, bar codes, etc.
- Mobile Device Management
  - Controls and monitors a device remotely
- Device Access Control
  - Lock screens, etc.
  - Device should be unlocked to access USB / Bluetooth
- Removable Storage
  - Devices support microSD cards
  - Can also support external storage
  - Sometimes Bluetooth and Wi-Fi based storage too
- Disabling Unused Features
  - Lessens the chance of exploitation

- Application Security
  - Key Management
    - Key generation
      - Mobile devices have poor RNGs
    - Key storage
      - Use Trusted Platform Module
      - Use Removable Hardware
  - Credential Management

    - Password managers with multifactor authentication
- Authentication
    - Methods
        - Patterns
        - PINs
        - Biometrics
        - RFID
    - Encryption when locked
- Geotagging
    - Embedding of location and data time on photos
    - Can disclose your location when photo is uploaded
- Encryption
    - Prevents access to data in storage or transit
    - Natively available on devices
    - Can also be implemented via apps
- Application Whitelisting
    - Allows only a specific list of apps to be installed
    - Implicit deny
- BYOD Concerns
    - Devices can access the company network
    - They need to comply with security policies
- Data Ownership
    - Personal and company data might be mixed in the device
    - They should be segmented
    - Policy should define who owns what data
- Support Ownership
    - Responsibility for repair and maintenance
- Patch Management
    - Responsibility for installing updates
    - How are updates to be installed
    - How frequent are updates to be installed
- Antivirus Management
    - What antivirus solution to use
    - Should an antivirus be used
- Forensics
    - Involvement of a device in investigations
- Privacy
    - Workers might be tracked when they are out of work
    - Contents of device may be monitored by the company
- On-boarding/Off-boarding

  - On-boarding
    - Installing security/management apps
    - Secure configuration
  - Off-boarding
    - Wiping business data
    - Full reset?
- Adherence to Corporate Policies
  - Personal mobile devices still need to comply with BYOD policies
- User Acceptance
  - BYOD policy details should be explained well to user
  - User must accept BYOD policy so they can be held accountable
- Architecture/Infrastructure Considerations
  - Allowing BYOD devices might cause more network load
  - Might require more IP addresses
  - Might require new hardware to be installed (access points)
- Legal Concerns
  - BYOD increases burden of liability
- Acceptable Use Policy
  - BYOD opens up inappropriate use of mobile devices
  - Risk of information disclosure is also increased
- On-board Camera/Video
  - Allows employees to take picture of company premises
  - Pictures of confidential information may be taken

- Cyber-Physical Systems
  - Limited functionality
  - May be part of a larger system/product
  - Examples
    - Static Systems
      - Does not change
      - Can't install new apps on it
      - Can't be configured
    - Network Enabled Devices
      - Devices that can communicate via networks
      - Wi-Fi, Ethernet, Bluetooth
    - Cyber Physical Systems
      - Can control physical components programmatically
      - Robots, doors, HVACs, self-driving cars, IoT, etc.
    - Mainframes
      - Usually designed around a single task
      - Might be considered static systems

      - Able to operate for decades
    - Game Consoles
      - OS is fixed and changed only when vendor releases a system upgrade
      - Focused on playing games and media
  - Methods of Securing
    - Network Segmentation
      - Isolate Cyber-Physical Systems in a separate VLAN
      - Prevents remote exploits
    - Security Layers
      - Isolating high security systems from lower security ones
      - Implementations
        - Physical Isolation
        - Network Isolation
        - etc.
    - Application Firewalls
      - Prevents application specific attacks
      - A server-side firewall
      - Use a network firewall as well
    - Manual Updates and Firmware Version Control
      - Ensures that updates are tested
      - Automatic updates allow for untested versions
      - This might lead to reduction in security
    - Wrappers
      - Encapsulates a solution or environment
      - Restricts and controls changes to an environment
      - Ensures that only valid and secure updates are applied
    - Control Redundancy and Diversity
      - Use multiple and redundant security controls
      - Fulfills defense in depth

Essential Security Protection Mechanisms

- Technical Mechanisms
  - Layering
    - Levels vs. Rings
      - Layering: Highest layer is most privileged
      - Rings: Lower ring is most privileged
    - Processes in different layers communicate via interfaces
    - Security policy set by higher privileged layers take precedence
  - Abstraction

- Generalizing a bunch of objects
- Hiding implementation details
- Only giving information on interfaces and attributes
- Allows setting of policies to groups of generalized objects

  - Data Hiding
    - Put objects in different container from subject
    - Ensure that object can only be accessed via a legal way
    - Hide data from processes running at different levels
    - Hide data from those who don't need to know and are unauthorized
  - Process Isolation
    - Each processes have their own memory spaces
    - Processes shouldn't be able to read each other's memory spaces
    - Prevents unauthorized data access
    - Protects integrity of a process as it can't be modified by another process without its consent
    - Implemented via sandboxing processes
  - Hardware Segmentation
    - Process isolation but uses hardware implementations for separation
    - Rare; used for national security concerns
- Policy Mechanisms
  - Least Privilege
    - Only give processes the privileges they need
    - Processes should run in user as much as possible
    - Use APIs to communicate with kernel mode processes instead
  - Separation of Privilege
    - Minimize the number of privileged operations a process can do
    - Basically, principle of least privilege for administrators
    - Compartmentalize responsibilities of processes
    - Prevents conflict of interest
  - Accountability
    - Record who does what
    - Requires authentication and authorization to associate activity with user
    - Allows users to be held accountable for their actions

Common Architecture Flaws

- Covert Channels
  - Allows unauthorized transmission of information
  - Detected by analyzing log files

  - Types
    - Covert Timing Channel
      - Modifies system's behavior to generate timing regularities
      - Observing system can then extract information by watching it
    - Covert Storage Channel
      - Writing data to a common storage area
- Coding Flaw Attacks
  - Initialization and Failure States
    - Security controls get unloaded when a system crashes
    - System crashes while it’s in privileged mode, giving attacker access
  - Input and Parameter Checking
    - Buffer Overflows: Length checking
    - Injection Attacks: Input sanitation and validation
  - Maintenance Hooks and Privileged Programs
    - Allows unauthorized privileged access
    - Allows bypassing of security controls
  - Incremental Attacks
    - Data Diddling
      - Making small random incremental changes to data
      - Difficult to detect
    - Salami Attack
      - Small whittling at assets like a salami
      - Transferring small amounts of cash from a compromised bank account over time
- Time of Check to Time of Use
  - Race condition
  - Object verified might be different from the one used
  - TOC - Time of Check
    - Process checks if the object is available and valid
    - Attack replaces object after the program checks it
  - TOU - Time of Use
    - Process then uses the object placed by attacked
  - Example:
    - Process: Check length of file
    - Attacker: Replace file with bigger one
    - Process: Reserves memory as large as the file that was read
    - Process: Leading the actual file into memory causes a buffer overflow
- Technology and Process Integration
  - Systems are being implemented via SOA
  - SOA integrates separate service applications into a single solution
  - Pay attention to Single Points of Failure

- Electromagnetic Radiation
    - EM leaks create a possible covert channel
    - Faraday Cage
        - Prevents radiation from going in and out of a bounded area
    - Jamming / Noise Generation
        - Creates meaningless radiation to prevent disclosure of information
    - Control Zones
        - Zone protected by jammers and faraday cages
        - A zone where not EM disclosure can occur

Physical Security Design

- There is no security without physical security
- Secure Facility Plan
    - Critical Path Analysis
        - Identifying mission critical assets/processes
        - Results in a list of items to secure
        - Technology Convergence must be considered
        - Technology Convergence
            - Tendency for technologies to merge over time
            - Results in single points of failure
            - Examples
                - Voice, Video, Fax, and Data uses single connection
                - Integrated Routers, Switches, and Firewalls
        - Example: E-Commerce Server
            - Internet Connection
            - Computer Hardware
            - Electricity
            - Temperature Control
            - Storage Faculty
        - Site Selection
        - Considerations
            - Visibility
                - Terrain
                - Visibility of Approaching Parties
            - Crime
                - Riots
                - Vandalism
                - Break-ins
            - Natural Disasters

        - Fault Lines
        - Tornadoes
        - Hurricanes
        - Flooding
    - Surrounding Businesses
        - Too Many Visitors
        - Noise
        - Vibrations
        - Dangerous Materials
    - Utilities
        - Fire Department
        - Medical
        - Police
- Faculty Design
- Considerations
    - Required Security Level
        - Forced Intrusions
        - Emergency Access
        - Resistance to Entry
        - Direction of Entries and Exits
        - Alarms
        - Conductivity
    - Safety
        - Fire Rating
        - Construction Materials
        - Load Rating
    - Access Control
        - Walls
        - Doors
        - Ceilings
        - Flooring
    - Utilities
        - HAVC
        - Power
        - Water
        - Sewage
        - Gas
- Secure Architecture
    - CPTED - Crime Prevention Through Environmental Design

Physical Security Implementation

- Categories of Physical Controls
    - Administrative
        - Facility Construction and Selection
        - Site Management
        - Personnel Controls
        - Awareness Training
        - Emergency Response and Procedures
    - Technical
        - Access Controls
        - Intrusion Detection
        - Alarms
        - CCTV
        - Monitoring
        - Heating
        - Ventilating
        - Air Conditioning
    - Physical
        - Fencing
        - Lighting
        - Locks
        - Construction Materials
        - Mantraps
        - Dogs
        - Guards
- Corporate v. Personal Property
    - Security controls should be placed where company assets are involved
    - Company is not responsible for safekeeping employee property
    - Company can be responsible for safekeeping key personnel and their property
- Functional Order of Controls
    - Deterrence
    - Make attackers think attacking is a bad idea
    - Example: Fencing
    - Denial
    - Prevent attackers from making an intrusion
    - Example: Vault Doors
    - Detection
    - Detect when an attacker has made an intrusion

    - Example: Motion Sensors
    - Delay
    - Make extraction of asset more difficult
    - Example: Cable Lock
- Equipment Failure
    - Considerations
        - Replacement part vendor
        - Transport and storage
        - Pre-purchasing
        - Installation and restoration skills
        - Scheduling maintenance and replacements
    - SLA - Service Level Agreement
        - Required response time from vendor to deliver a service
        - Includes repair, internet, hosting, etc.
        - Must be established with vendor for critical assets
    - MTTF - Mean Time to Failure
        - Time before a device fails
        - Expected lifetime of a device
        - Devices should be replaced before MTTF expires
    - MTTR - Mean Time to Repair
        - Time it takes to repair a device
    - MTBF - Mean Time Between Failures
        - Time between subsequent failures
        - Usually same with MTTF
- Wiring Closets
    - AKA, Premises Wire Distribution Room
    - Connects floor/building cables to essential equipment
    - Building management must be notified of wiring closet policies
    - Multiple wiring closets may exist for large buildings
        - To work around the maximum run length
        - Maximum run length is 100 meters
        - Run length is reduced in noisy environments
    - Houses wiring for other utilities as well:
        - Alarm systems
        - Circuit breakers
        - Telephone punch down blocks
        - Wireless access points
        - Security cameras
    - Rules
        - Do not use as storage area

        - Have adequate locks
        - Keep area tidy
        - Remove flammable items
        - Video surveillance
        - Door open sensor
        - Regular physical inspections
        - Include in environmental controls plan
- Server Rooms
    - Houses mission critical servers
    - Human Incompatibility
        - Fill room with halon substitutes
        - Low temperature
        - Little or no lighting
        - Equipment stacked with little room to maneuver
    - Location
        - At the center of the building
        - Away from sewage lines, water, and gas
    - Walls
        - One hour minimum fire rating
- Media Storage Facilities
    - Stores blank and reusable media
    - Threats
        - Theft
            - Restrict Access to Media
            - Asset Tracking (RFID/NFC)
        - Malware Planting
            - Sanitize Returned Media
            - Restrict Access to Media
        - Data Remnant Recovery
            - Secure Data Wiping
            - Restrict Access to Media
        - Destruction
            - Fire
            - Flood
            - Electromagnetic Field
            - Temperature Monitoring
    - Data Remnants
        - Remaining data on storage left over after deletion
        - Deletion only removes file record
        - Doesn't remove actual file data from disk

        - Can be recovered using un-delete utilities
    - Restricting Access to Media
        - Use a locked cabinet or safe
        - Check in and check out procedure
        - Have a custodian who manages access
- Evidence Storage
    - Stores evidence after breach
    - Requirements
        - Dedicated storage system/network
        - Keeping storage system offline
        - Block internet connectivity
        - Tracking all activities on system
        - Calculating hashes for all datasets within
        - Limiting access to security administrator
        - Encrypting all datasets stored within
- Work Area Security
    - Controls
        - Separate work areas and visitor areas
        - Escort requirements for visitors
        - Require badges and RFID tags
        - More restrictive access to more sensitive areas
        - Sensitive areas should be in the center of facility protection
        - Universal access to essential facilities (e.g. restrooms)
        - Work area sensitivity classifications
        - Walls / Partitions
            - Prevents shoulder surfing or eavesdropping
            - Walls should cut off false ceilings
                - For separating areas with different sensitivity
- Data Center Security
    - Usually the same as server rooms
    - Same policies as server rooms
    - Might be a separate building or remote location
    - Might be leased
    - Technical Controls
        - Smartcards
            - Types
                - Magnetic Strip
                - Bar Code
                - Integrated Circuit Chip
            - Threats

        - Social Engineering
        - Theft
    - Should come with 2-factor authentication (e.g. PIN)
    - Examples: Memory Cards
        - Machine readable ID cards with magnetic strip
- Proximity Readers
    - Passive
        - Alters reader EM field
        - No electronics
        - Just a small magnet
    - Field Powered
        - Uses reader EM field for power
        - Must be waved near reader
    - Transponder
        - Self-powered
        - Transmits signal received by reader
        - Occurs consistently or at press of button
- Intrusion Detection Systems
    - Detects attempted intrusions
    - Used to raise an alarm
    - Points of Failure
        - Power
            - Lack of power prevents the system from operating
        - Communication
            - Lack of communication prevents alarm from being raised
    - Controls
        - Heart Beat Sensor
            - Periodically tests connectivity between alarm and IDS
            - Alarm is raised if heartbeat signal fails
- Access Abuses
    - Examples
        - Opening Secured Doors
        - Bypassing Locks and Access
        - Masquerading
            - Using someone else's security ID
        - Piggybacking
            - Following someone through a secured gate
    - Controls
        - Audit Trails
            - Can be manually or automatically generated

    - Emanation Security
        - Sources
            - Wireless Networking Equipment
            - Mobile Phones
        - TEMPEST
            - Government research
            - For protecting equipment against EMP
            - Expanded to monitoring emanations
        - Controls
            - Faraday Cage
                - Box fully surrounded by a wire mesh
                - Prevents EM signals from entering an existing enclosure
            - White Noise
                - False traffic to hide presence of real emanations
                - Real signal from another source can be used
                - Used around the perimeter of an area
            - Control Zone
                - A zone protected by a Faraday cage or white noise
                - Can be a room, floor, or building
- Utilities and HVAC
    - Power Issues
        - Terms
            - Fault
                - Momentary loss of power
            - Blackout
                - Prolonged loss of power
            - Sag
                - Momentary low voltage
            - Brownout
                - Prolonged low voltage
            - Spike
                - Momentary high voltage
            - Surge
                - Prolonged high voltage
            - Inrush
                - Initial surge of power when connecting to source
            - Transient
                - Momentary power fluctuation
            - Noise
                - Prolonged power fluctuation
            - Clean

            - Non fluctuating power
        - Ground
            - The wire in a circuit that is grounded
    - Controls
        - UPS - Uninterruptable Power Supply
            - Sanitizes power
            - Provides power for a few minutes
        - Power Strips + Surge Protectors
            - Fuse blows when damaging power levels occurs
        - Power Generators
            - Provides power until main power comes back on
- Noise Issues
    - Generated by electric current
    - Affects quality of communications
    - EMI - Electromagnetic Interference
        - Common Mode Noise
            - From difference in power between hot and ground wires
        - Traverse Mode Noise
            - From difference in power between hot and neutral wires
    - RFI - Radio Frequency Interference
        - Generated by common electrical appliances
        - Microwaves, lights, heaters, computers
    - Controls
        - Shielding
        - Grounding
        - Power Conditioning
        - Limiting RFI and EMI exposure
- Temperature, Humidity, and Static
    - Temperature
        - 60F to 70F
        - 15C to 23C
    - Humidity
        - 40% to 60%
        - Too Much: Corrosion
        - Too Low: Static
- Water Issues
    - Threats
        - Leakage
        - Flooding
        - Electrocution
    - Controls

- Monitor plumbing for leaks
- Ensure water is away from electricity
- Ensure servers are away from water
- Ensure the facility is away from flooding areas

- Fire Prevention, Detection, and Suppression
  - Fire Triangle
    - Heat
    - Oxygen
    - Fuel
    - Chemical Reaction
  - Stages of Fire
    - Incipient
      - Air ionization; No smoke
    - Smoke
      - Smoke is visible from point of ignition
    - Flame
      - Flame can be seen with naked eye
    - Heat
      - Heat buildup and fire spreads
  - Suppression Mediums
    - Water
      - Suppresses heat
    - Soda Acid / Dry Powders
      - Suppresses fuel
    - CO2
      - Suppresses oxygen
    - Halon Substitutes / Nonflammable Gases
      - Suppresses reaction
  - Controls
    - Training
    - Emergency Shutdown Procedures
    - Rendezvous Location
    - Safety Verification Mechanism
  - Fire Extinguishers
    - A - Wood/Paper - Water, Soda Acid
    - B - Oils/Liquids - CO2/Halon/Soda Acid
      - Splashes when doused
    - C - Electrical - CO2/Halon
      - Electrocution
    - D - Metal - Dry Powder
      - Produces own oxygen

- Detection Systems
    - Types
        - Fixed Temperature
            - Metal/plastic which melts at a temperature
        - Rate-of-Rise
            - Monitors speed of temperature change
        - Flame-Actuated Systems
            - Monitors infrared energy
        - Smoke-Actuated Systems
            - Photoelectric / radioactive ionization
- Suppression
    - Water Suppression
        - For human friendly environments
        - Types
            - Wet Pipe / Closed Head
                - Pipe is always full of water
            - Dry Pipe
                - Water is filled with gas and is discharged
            - Deluge
                - Large pipes; large volumes of water
            - Preaction
                - Dry pipe until fire is detected
                - Has a secondary trigger which releases water
                - Allows fire to be dealt with before activating
                - Good for areas with electronics and humans
    - Gas Discharge Systems
        - For human incompatible environments
        - Degrades into toxic gas
        - Halon is now banned by the EPA
        - Types
            - Halon
            - FM-200 (HFC-227ea)
            - CEA-410 / CEA-308
            - NAF-S-III (HCFC Blend A)
            - FE-13 (HCFC-23)
            - Argon (IG55) or Aragonite (IG01)
            - Intergern (IG541)
            - Low Pressure Water Mists
- Damage
    - Smoke
        - Smoke from a fire can damage storage devices

      - Heat
        - Heat from a fire can damage storage tapes and hardware
      - Suppression
        - Suppression mechanism can damage equipment
        - Water and soda acid damages computers
        - Can cause short circuits and corrosion
      - Fire Department
        - May damage equipment and walls using axes
        - May damage using chosen fire suppression

Physical Security Management

- Perimeter
  - Accessibility
    - Entrances
      - Single Entrance
        - For security
      - Multiple Entrances
        - For emergencies
    - Roads and Transportation
    - Constrained by perimeter security
  - Controls
    - Fence
      - Defines a security perimeter
      - Deterrent levels
        - Vs. Casual Trespassers
          - 3 to 4 feet
        - Vs. Most Trespassers
          - 6 to 7 feet
        - Vs. Determined Trespassers
          - 8 feet or more
          - With barbed wire
    - Gate
      - Controlled entry and exit point
      - Must match deterrent level of fence
      - Must be hardened vs tampering/removal/destruction
      - Must not offer access when closed
      - Number must be kept to a minimum
      - Must be protected by guards or CCTV
    - Turnstile

      - Prevents tailgating
      - Allows one person at a time
      - Allows movement in 1 direction
      - Used for entry rather than exit
    - Mantrap
      - Double set of doors
      - Protected by a guard
      - Prevents piggybacking or tailgating (e.g. weight measurement)
      - Immobilizes a subject until authenticated
      - If unauthenticated, subject is locked until authorities respond
    - Lighting
      - Discourages casual intruders
      - Not a strong deterrent
      - Should not show positions of detection controls
      - Should not cause glare to detection controls
      - Should illuminate critical areas w/ 2 candle feet of power
      - Should be placed apart as their illumination diameter
    - Guards and Dogs
      - Advantages
        - Can adjust to changing environment
        - Can detect and respond to threats
        - Acts as a deterrent
      - Disadvantages
        - Cannot be posted in human incompatible locations
        - No guarantees of reliability
        - Can be subject to injury or sickness
        - Vulnerable to social engineering
        - Protection stops when life is endangered
        - Not aware of the scope of operations of facility
        - Expensive
- Internal Security
  - Controls
    - Visitor Control
      - Escorts
      - Monitoring
    - Locks
      - Key / Preset Locks
        - Vulnerable to picking / shimming
        - Key can be lost
      - Combination

        - Combination can be forgotten
        - Can include electronic controls
        - Can include multiple valid combinations
- Badges
    - Identification cards
    - Can be visual/smartcard/both
    - Can be used to authenticate to facility
    - Authenticated by security guards or scanning devices
    - May require other authentication factors
- Motion Detectors
    - Detects movement or sound in an area
    - Types
        - Infrared
            - Detects changes in infrared lighting
        - Heat-based
            - Detects changes in heat levels
        - Wave-pattern
            - Transmits signal into area
            - Detects changes in reflected pattern
        - Capacitance
            - Detects changes in electrical field
        - Photoelectric
            - Detects changes in visible light patterns
        - Passive Audio
            - Detects abnormal sound in area
- Intrusion Alarms
    - Triggered by a sensor
    - By Mechanism
        - Deterrent Alarm
            - Engages additional locks or shuts down doors
            - Makes attack more difficult
        - Repellant Alarm
            - Triggers siren and lights
            - Meant to discourage attackers
            - Forces them off premises
        - Notification Alarm
            - Sends a notification to guards
            - Usually silent
            - Allows security to capture intruder
    - By Location
        - Local Alarm

          - Audible alarm
          - Can be heard for 400 feet
          - Locally positioned guards must be able to respond
          - Must be protected from tampering
        - Central Station Systems
          - Notifies a central station
          - Locally silent
          - Usually well-known security companies
          - Examples: Residential security systems
          - Proprietary System
            - Central station system used by private companies
        - Auxiliary Station
          - Alarm which notifies emergency services
          - E.g. police/fire/medical
          - Can be added to local alarms and central station systems
      - Secondary Verification
        - Used to verify if alarm was valid
        - Examples
          - Multiple Sensor Systems
            - Must be triggered in quick succession
          - CCTV
            - Allows guards to manually verify area
- Safety
  - Life
    - Protecting human life is the first priority of security
    - Includes providing them with means to survive during disasters
    - E.g. food, water, etc.
  - Environment
    - Ensuring that environment remains safe during disaster
    - Deals with flooding, fires, toxic gas, etc.
  - Occupant Emergency Plans
    - Sustains personnel safety in the wake of a disaster
    - How to minimize threats to life and prevent injury
    - Does not address IT issues
- Privacy and Legal
  - Privacy
    - Protecting personal information from disclosure
    - Personal information includes:
      - Name

        - Address
        - Phone
        - Race
        - Religion
        - Age
- Regulatory Requirements
    - Depends on industry
    - Regulatory requirements must be considered a baseline for security