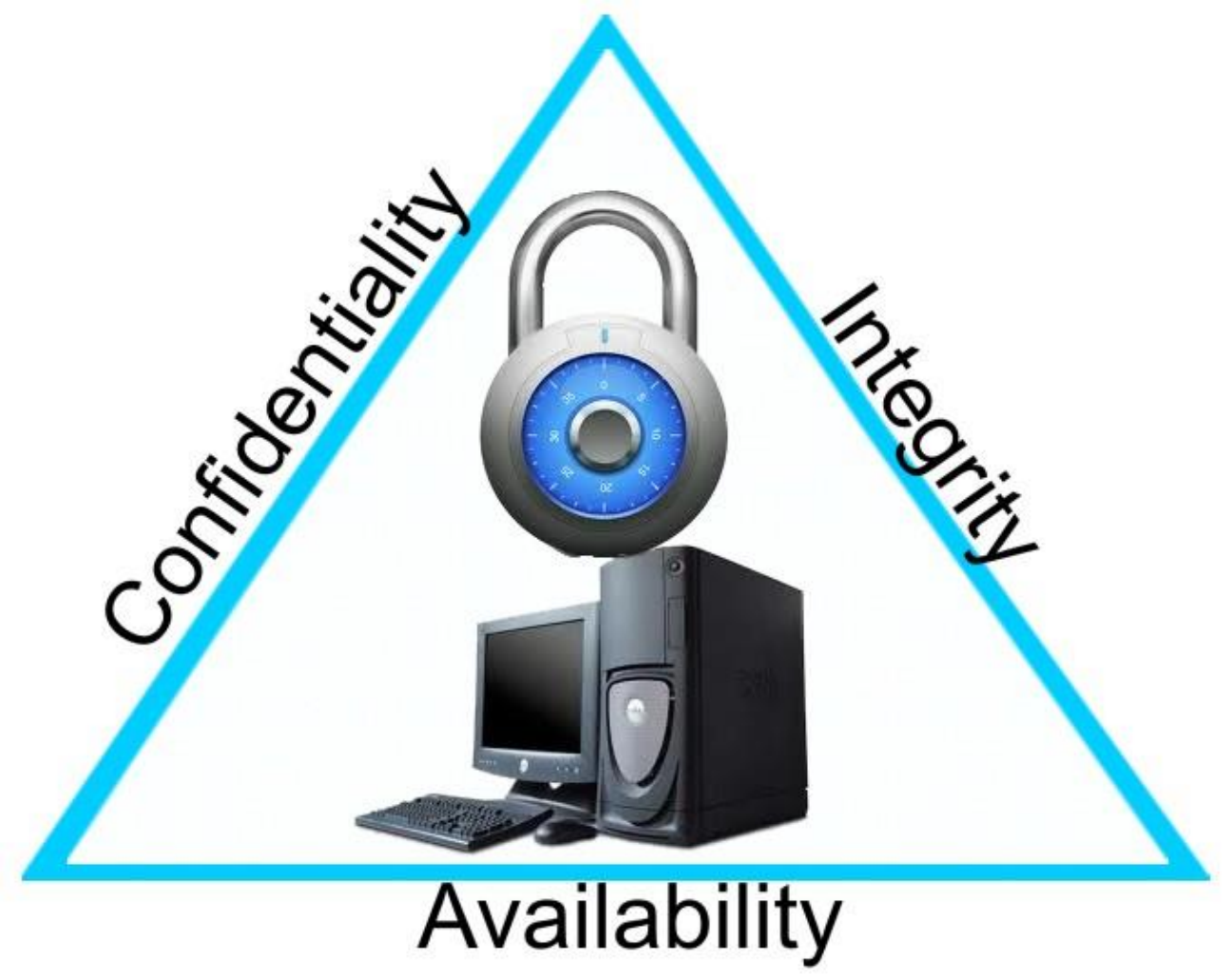
Security and Risk Management

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

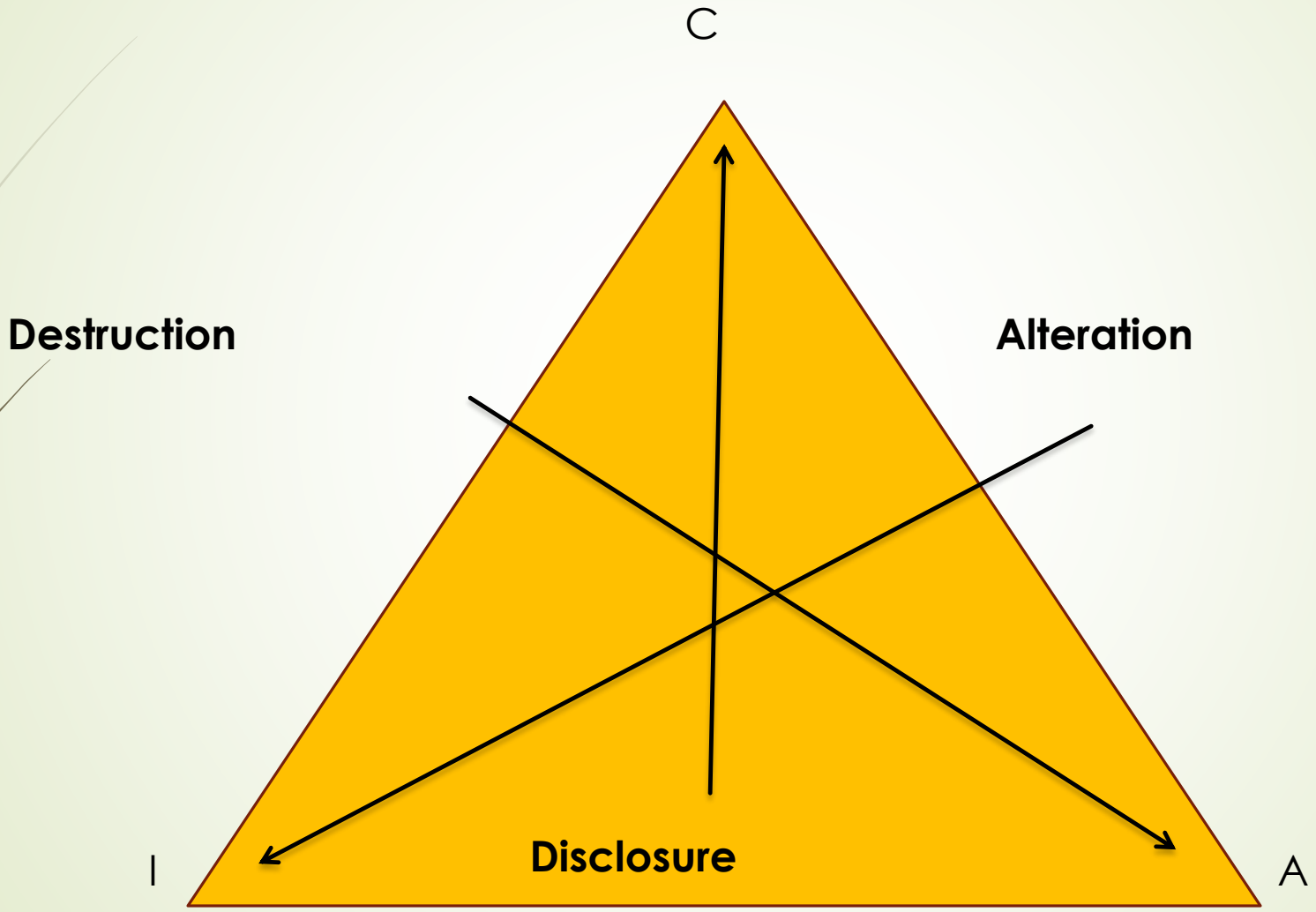
Domain Objectives

- Understand and apply concepts of confidentiality, integrity, and availability
- Apply security governance principles through compliance
- Understand legal and regulatory issues that pertain to information security in a global context
- Develop and implement documented security policy, standards, procedures, and guidelines
- Understand business continuity requirements
- Contribute to personnel security policies
- Understand and apply risk management concepts
- Understand and apply threat modeling
- Integrate security risk considerations into acquisitions strategy and practice
- Establish and manage security education, training, and awareness

The CIA Triad



Disclosure, Alteration, Destruction



Confidentiality

- Protection from
  - Unauthorized access
  - Unauthorized use
  - Disclosure
- Protect data
  - Residing on systems
  - In transit
  - In process

Confidentiality

- **Threats**
  - **Sniffing**
  - **Stealing password files**
  - **Social engineering**
  - **Shoulder surfing**
  - **Eavesdropping**
  - **Poor user training/awareness**
  - **Disclosure**

- Countermeasures
  - Encryption
  - Traffic padding
  - Access controls
  - Authentication
  - Data classification
  - Personnel training
  - Shielding

Integrity

- Provides assurance of accuracy and reliability
- Ensures objects retain their veracity
- Modifications by authorized subjects only
- Detects alterations that have occurred
  - In storage
  - In transit
  - In process

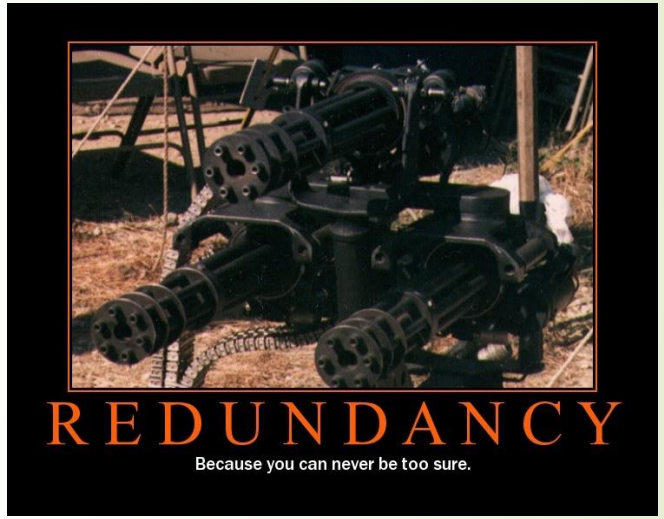
Integrity

- Attacks on Integrity
  - Viruses
  - Logic bombs
  - Unauthorized access
  - Coding errors
  - Malicious modifications
  - Data diddling
  - System back doors
  - Human error, oversight, or ineptitude
  - Alteration

- Countermeasures
  - Strict access controls
  - Rigorous authentication procedures
  - Intrusion detection systems
  - Object/data encryption
  - Hash total verifications
  - Interface restrictions
  - Input/function checks
  - Extensive personnel training

Availability

- Controls ensure:
  - Authorized access
  - Acceptable level of performance
  - Fault tolerance
  - Redundancy
  - Reliable backups
  - Prevention of data loss or destruction



Availability

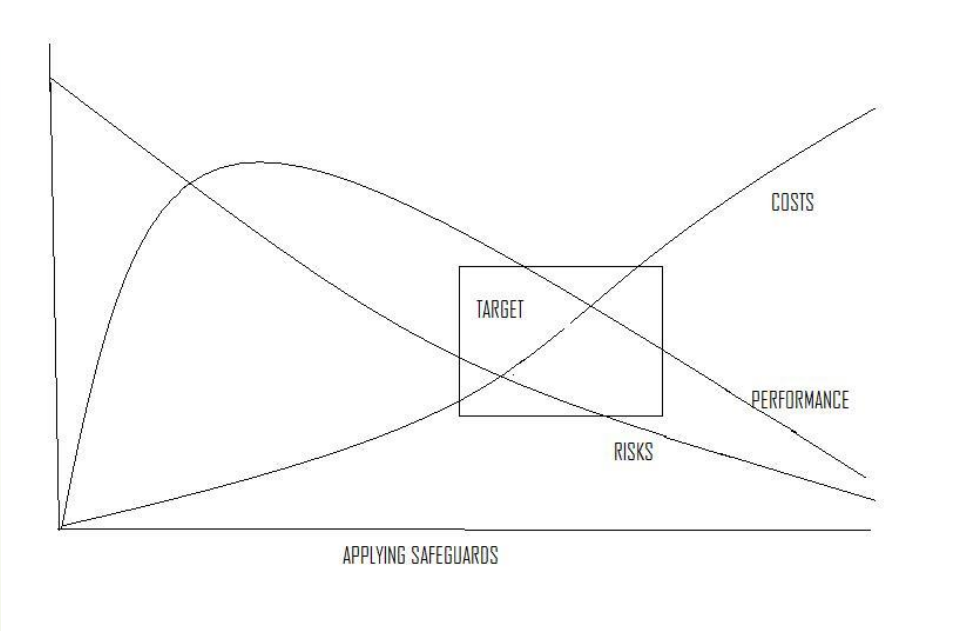
- Threats
  - Device failure
  - Destruction
  - Software errors
  - Environmental issues
  - Attacks
    - DoS
    - Object destruction
    - Communication interruptions
    - Human error, oversight, or ineptitude
- Countermeasures
  - Proper systems design
  - Software design and testing
  - Effective access controls
  - Monitoring performance & network traffic
  - Perimeter security devices
  - Implementing redundancy
  - Maintaining & testing backups

Tension Between the Concepts

- **Confidentiality, Integrity, and Availability are often at odds with each other**

- **The security mission is to find balance between the concepts**

"The food is just so-so, but the security is fantastic."



Threats to Operations

- Disclosure
- Destruction
- Interruption/Non Availability
- Corruption/Modification
- Theft
- Espionage
- Hackers / Crackers
- Malicious Code

IT Governance

- **IT Governance Institute (ITGI)**

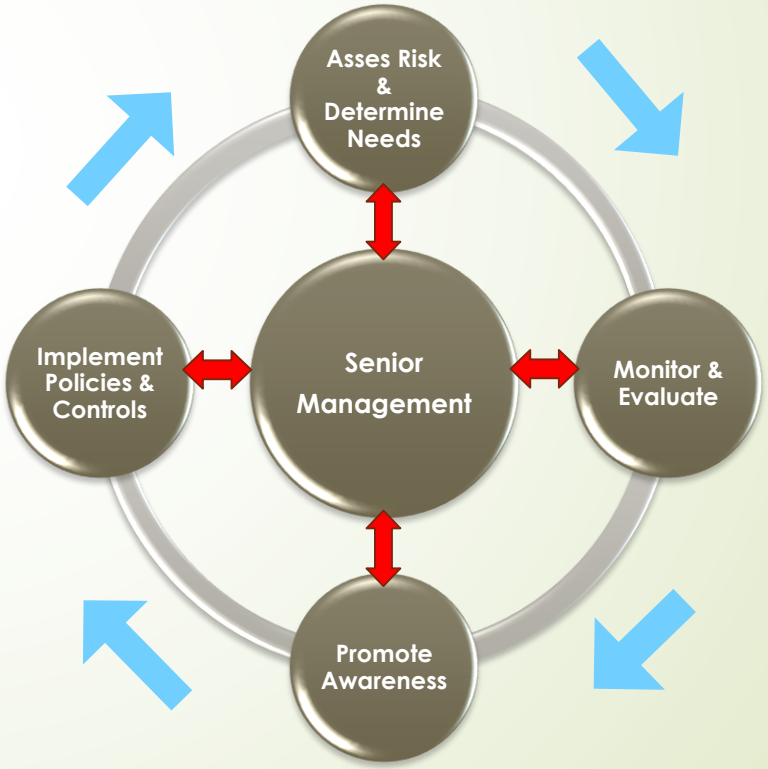
- **Definition: "the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives"**

Governance Committees

- **Responsible for recruiting and maintaining the governance board**
- **Responsible for determining missing qualifications and characteristics of board members**

Security Management Practices

- Organizational assets are protected through the implementation of:
  - Physical controls
  - Administrative controls
  - Managerial controls
  - Technical controls
  - Operational controls



Security Management

- Responsibilities
  - Starts with the Senior Management
  - Scope has to be clearly defined
  - Actual goals are identified
  - Evaluation of:
    - Business objectives
    - Security risks
    - User productivity
    - Functionality requirements

Security Management

- Must
  - Properly identify and value assets
  - Implement security
    - Policies
    - Procedures
    - Standards
    - Guidelines / Baselines
  - Provide
    - Confidentiality
    - Integrity
    - Availability

Acquisitions and Mergers

- Plan for:
  - New data types requiring differing levels of protection
  - New technology types that need differing protection
  - New staff and roles
  - Inherited threats
  - New vulnerabilities
  - Potential new policies
  - New external business partners and interconnections

Divestitures and Spinoffs

- Plan for:
  - Data loss and leakage due to employee loss
  - Unsecured ports and interconnections
  - Loss of network/log visibility
  - New threats from former employees
  - Need to revise policies, standards, and procedures
  - Need to meet deadlines for data segregation

Creating Roles

- **Establishing clear, unambiguous security roles has many benefits to the organization beyond providing information as to the responsibilities to be performed and who needs to perform them. These benefits include:**
  - **Demonstrable executive management support for information security**
  - **Lower risks to company reputation/ brand recognition due to security problems**
  - **Personal accountability for information security**

Roles & Responsibilities

- Senior Manager
  - Decision makers
  - Due care & due diligence
- Security Professional
  - Implementers
- Data Owner
  - Classification of data
- Data Custodian
  - Maintain and protect the data
- User
  - Least Privilege
- Auditor
  - Provides compliance and effectiveness reports

Information Security Officer

- Is responsible for:
  - Ensuring the protection of all of the business information assets from intentional and unintentional loss, disclosure, alteration, destruction, and unavailability
  - Acts as the facilitator of information security for the organization
  - Ensuring that the security policies, procedures, baselines, standards, and guidelines are written to address the information security needs of the organization
  - Stay abreast of emerging technologies and threats
  - Compliance
  - Implementing incident response capabilities
  - Information security awareness program
  - Understanding the vision, mission, objectives/ goals, and plans of the organization

Communicating Risks to Executive Management

- **The Security Officer should clearly presented all facts and provide information that is based upon a real business need or is tied to a business objective**
- **Recommendations for specific controls should be risk based**
- **Presentations should be geared at a high level to convey the purpose of the technical safeguard**

Reporting Model

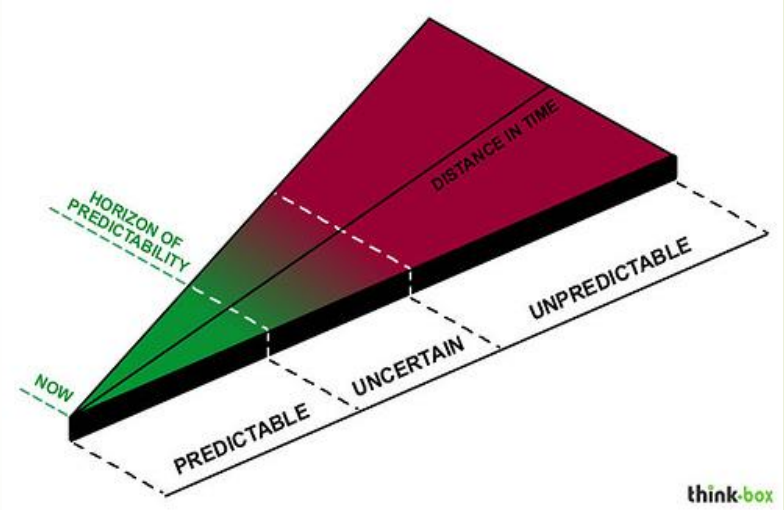
- Report as high as possible to:
  - Maintain visibility of the importance of information security
  - Limit the distortion or inaccurate translation of messages that can occur due to hierarchical, deep organizations
- Reporting directly to the CEO
  - Reduces filtering of messages
  - Demonstrates importance of information security

Budgeting

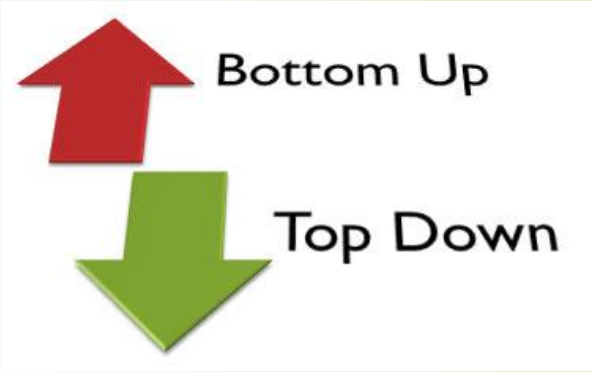
- Security should be included in other department budgets
- Planned security is cheaper than when adding it as an afterthought
- Security should be considered into project costs during each phase of development
- Proper budgeting is accomplished by combining risk analysis, TCO and ROI calculations
- Areas to consider when budgeting:
  - Application security
  - Configuration change management
  - Finances
  - Incident management
  - Patch management
  - Vulnerability management

Security Planning

- Strategic Plan
  - Long term & stable
  - Period of 5 years
- Tactical Plan
  - Midterm & detailed
  - Period of 1 year
- Operational Plan
  - Short-term & highly detailed
  - Updated regularly



Security Management Planning



- Top Down Approach
- Upper/Senior Management
  - Defines policies
- Middle Management
  - Creates standards, baselines, guidelines, & procedures
- Operational Managers/Security Professionals
  - Implement
- End Users
  - Comply

Security Council

- Vision statement
  - Draws upon the security concepts of CIA to support the business objective
  - Nontechnical, brief, to the point and achievable
- Mission statement
  - Objectives that support the overall vision
  - Goals, initiatives, objectives to achieve vision

Security Program Oversight

- Helps to guide and support the information security program
- Decide on Project Initiatives
- Prioritize Information Security Efforts
- Review and Recommend Security Policies
- Review and Audit the Security Program
- Champion Organizational Security Efforts
- Recommend Areas Requiring Investment

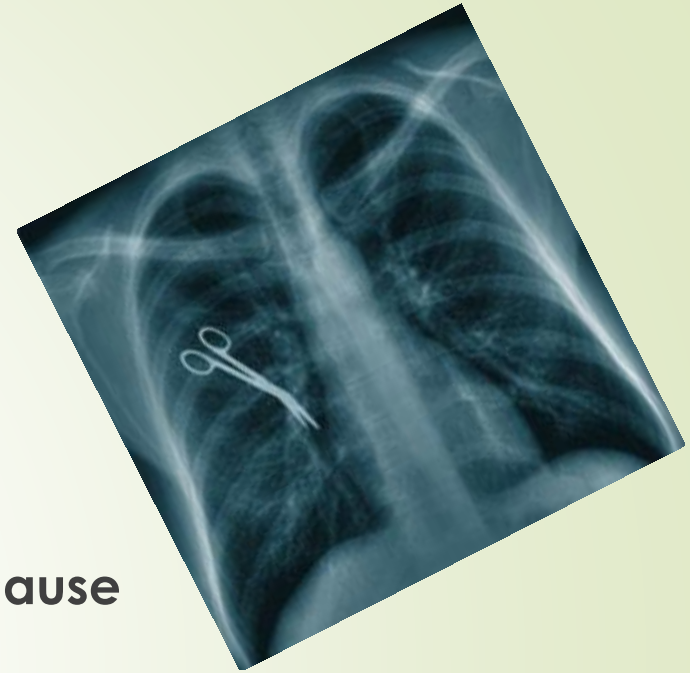
Control Frameworks

- Control frameworks aid an organization's governance efforts by:
- Providing consistency
- Providing assessment standards or procedures
- Relying on standardization
- Comprehensive coverage of legal and regulatory requirements
- Being modular to withstand change and modification

Due Care/Due Diligence

- Due Care
  - Do what a reasonable person would do (prudent man rule)
  - Informal (passive)
  - “duty of care”
- Due Diligence
  - Management of due care
  - A step beyond due care
  - Active

Liability - Negligence



- Liability
  - Legal Responsibilities
  - Penalties
  - Negligence: recognized obligation / proximate cause
    - Due Care (Passive)
    - Due Diligence (Active)
    - Downstream Liabilities
    - Prudent Man Rule
- Gross Negligence
  - Opposite of Due Care
  - Negligence can be legally found if the due care was not performed

Governance, Risk Management, and Compliance (GRC)

- **Purpose: analyze risks and manage mitigation in alignment with business and compliance objectives.**
- **GRC ensures than an organization acts in accordance with internal rules, acceptable levels of risk, and external regulations**
- **Generally the focus is on compliance first and then expanded to include risk management and governance.**

European Union Privacy

- EU Data Protection Directive
  - Notify individuals on how their data is collected and used
  - Allow individuals to opt out of sharing personal data with third parties
  - Require individuals to opt into sharing the most sensitive data with third parties
  - Provide reasonable protection for personal data

- EU-US Safe Harbor
  - EU citizen personal data can not be transmitted, even with permission of the individual, outside of the EU
  - Safe Harbor allows US companies to pass data
  - American companies doing business in Europe can obtain protection under a treaty between the European Union and the United States that allows the Department of Commerce to certify businesses that comply with regulations and offer them "Safe Harbor" from prosecution

Categories of Computer Crime

- **Computer-assisted**
- **Computer-targeted**
- **Computer is incidental**

The Effects of Cybercrime

- Loss of intellectual property or sensitive data
- Damage to brand image and reputation
- Opportunity costs such as service and employment disruptions
- Penalties and compensatory payments
- Insurance and countermeasure costs
- Costs of mitigation and recovery

Intellectual Property Protection

- Types of intellectual property
  - Industrial property
    - Patent
    - Trademarks
    - Industrial designs
  - Copyright
    - Novels
    - Plays
    - Films
    - Music
    - Photographs
    - sculptures

Intellectual Property Protection

- Patent
  - Strongest form of intellectual property protection
  - Good for 20 years
  - Inventor granted exclusive rights during patent period
  - The invention must be new (novel)
  - The invention must be useful
  - The invention must not be obvious
  - Obtaining a patent in one country, does not give the owner of the patent worldwide protection for the invention

Intellectual Property Protection

- Trademark
  - Good for 10 years
  - Does not have to be registered with the US Patent and Trademark Office to be protected by law
  - To protect your trade mark throughout the European Community, you can apply for a community trade mark (CTM) via the Office for Harmonization in the Internal Market (OHIM)
  - World Intellectual Property Organization (WIPO) oversees international trademark efforts

- Trademark attacks:
  - Counterfeiting
  - Dilution
  - Cyber squatting
  - Typo squatting

Intellectual Property Protection

- Copyright
  - In effect for author's life plus 50 years (US law is 70 years)
  - Corporate authorship is the shorter of 95 years from publication or 120 years from completion
  - Upon expiration a copyrighted item becomes public domain.
  - Some high value copyrights have had extensions if the loss of copyright presented a large financial loss
  - First Sale and Fair Use Doctrine

- Copyright attacks:
  - Software piracy
  - Copyright infringement

Intellectual Property Protection

- Trade Secret
  - Intellectual property that is absolutely critical to a business
  - Protection is solely the responsibility of the business
  - Commonly protected by non-compete or non-disclosure agreements
  - Lasts forever unless it becomes public knowledge by some legal means
- Trade secret attacks:
  - Corporate espionage

Information Technology Licensing

- Four categories of software licensing
  - Freeware, shareware, commercial, and academic

- Intellectual Property Laws
  - Licensing Issues
    - Contractual, Shrink-wrap, Click-wrap
    - Uniform Computer Information Transactions Act
  - Software Piracy
    - Software Protection Association (SPA)
    - Business Software Alliance (BSA)
    - Federation Against Software Theft (FAST)

Import and Export Restrictions

- Import/export laws were created because of concerns about new information technologies and products with military applications being transferred outside of the USA
- International Traffic In Arms Regulation (ITAR)
  - Controls the import/export of items considered defense articles and defense services
- Export Administration Regulations (EAR)
  - Allows the President to regulate the export of civilian goods and technologies that have military applications
- Wassenaar Arrangement (post cold war):
  - Standard for export controls
  - Restricts access to countries not included in arrangement

Trans-Border Data Flow

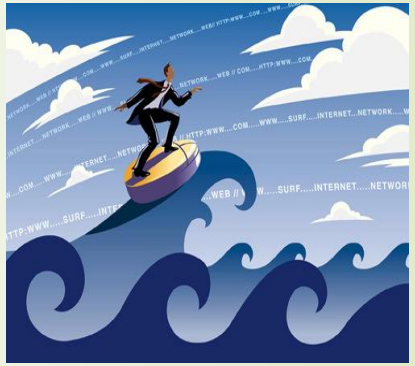
- Issues:
  - Identify citizens and visitors to fight terrorism, combat fraud, and deliver services
  - Reduce costs, become more efficient, outsourcing
  - Data retention across various jurisdictions
  - Information rights and privacy
  - Differing data protection legislation

Organization for Economic Cooperation and Development (OECD) Privacy Guidelines

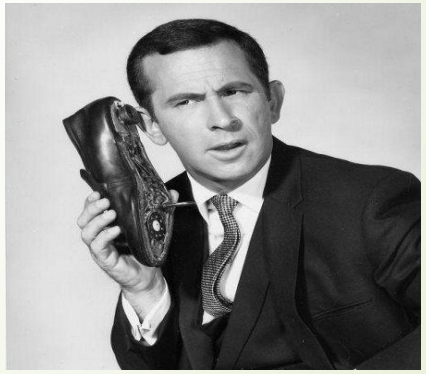
- Organization for Economic Cooperation and Development
- 30 member nations
- Based on 8 core principles or guidelines which form the minimum set of requirements for the development of reasonable legislation, regulations and policies
- Cautions members to be aware of and sensitive to regional or domestic differences and to safeguard personal information from countries that do not follow their guidelines or an equivalent

Privacy

- Addressed in the organization security policy
  - Individual vs. Organization
  - Email policy
  - Recording phone conversations
  - Surfing



- Personally Identifiable Information (PII):
  - Online visitors
  - Customers
  - Employees
  - Suppliers
  - Contractors



Data Breaches

- Incident
  - Security event that compromises the integrity, confidentiality or availability of an information asset
- Breach
  - Incident that results in disclosure or potential exposure of data
- Data Disclosure
  - Breach for which it was confirmed that data was actually disclosed to an unauthorized party
- US Breach Notification Laws are at the state level
  - Purpose: to notify an individual that his personal information has been compromised

Vocabulary for Recording and Incident Sharing (VERIS)

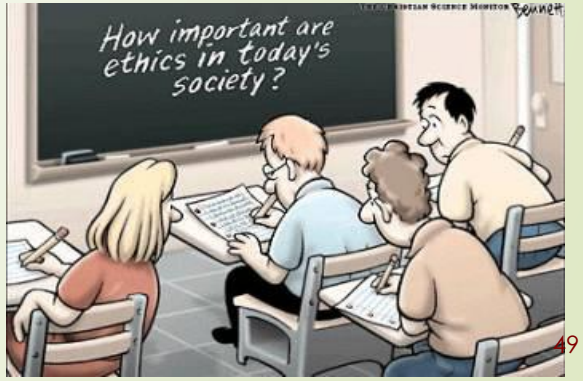
- **Provides a common language for describing security incidents**

- **VERIS Community Data Base (VCDB)**
  - **Records all publicly disclosed security incidents in a free and open dataset**
  - **www.vcdb.org**

(ISC)^2 Code of Ethics

- Code of Ethics Preamble
  - Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior
  - Therefore, strict adherence to this code is a condition of certification

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



Ethics and the Internet

- Internet Architecture Board (IAB)
  - Committee charged with the oversight of the technical and engineering development of the Internet (RFC 1087)

- Computer Ethics Institute (CEI)
  - Nonprofit organization focused on the issues, dilemmas and challenges of advancing IT within ethical frameworks
  - Ten Commandments of Computer Ethics

Ethics Fallacies

- Computer Game Fallacy
- Law-Abiding Citizen Fallacy
- Shatterproof Fallacy
- Candy-From-A-Baby Fallacy
- Hacker Fallacy
- Free Information Fallacy

Hacker Ethic

- Computer access should be unlimited and total
- All information should be free
- Authority should be distrusted and decentralization promoted
- Hackers should be judged solely by their skills
- Computers can be used to create art and beauty
- Computers can change your life for the better

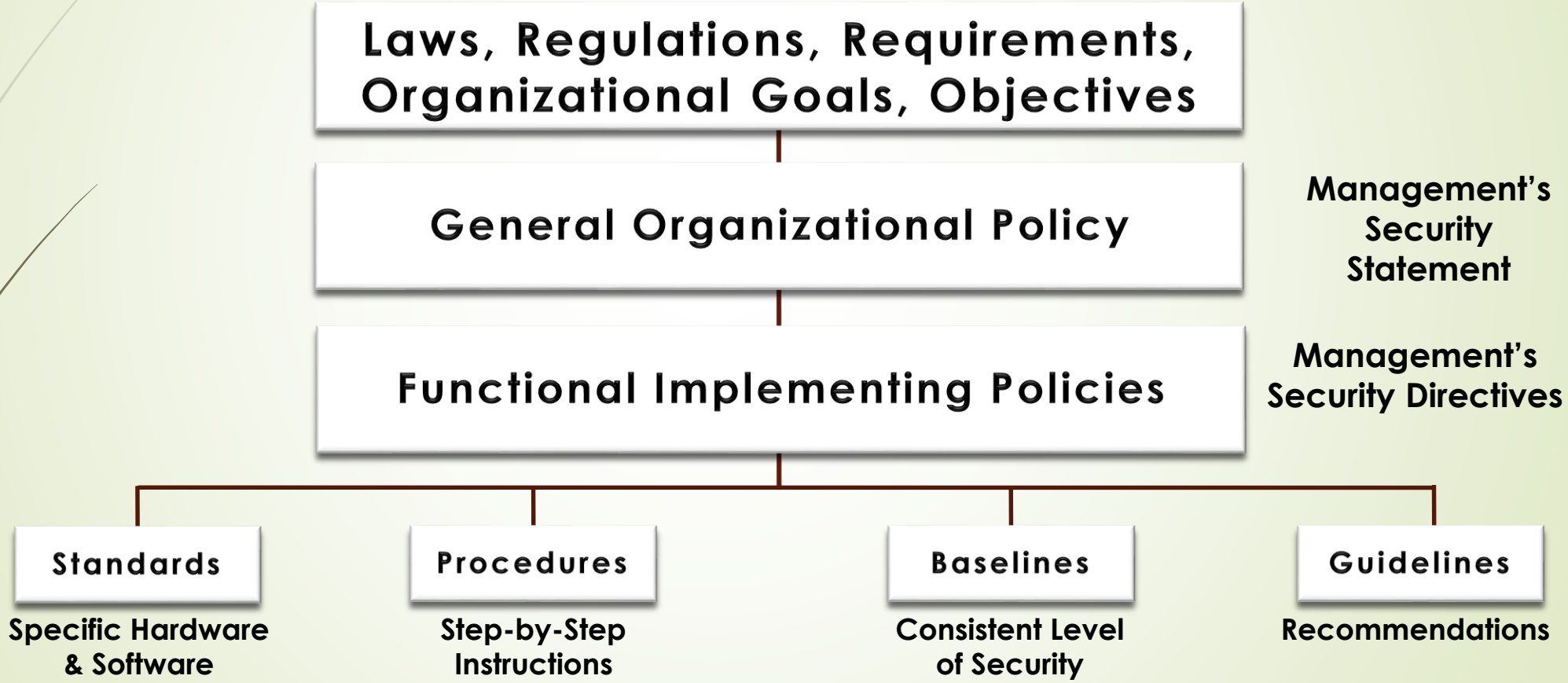
Ethical Bases for IT Decision Making

- Golden Rule
- Kant's Categorical Imperative
- Descartes' rule of change (slippery slope)
- Utilitarian Principle
- Risk aversion Principle
- Avoid Harm
- No Free Lunch Rule
- Legalism
- Professionalism
- Evidentiary Guidance
- Client/Customer/patient Choice
- Equity
- Competition
- Compassion/Last Chance
- Impartiality/Objectivity
- Openness/Full Disclosure
- Confidentiality
- Trustworthiness and Honesty

Ethical Principles for Processing Information in the Workplace

- Informed consent
- Higher Ethic in the Worst Case
- Change of Scale Test
- Owners' Conservation of Ownership
- Users' Conservation of Ownership

Relationship among Policies, Procedures, Standards, Baselines, and Guidelines



Policies, Standards, Baselines, Guidelines, and Procedures

- Policies
  - Broad overviews
- Standards
  - Compulsory requirements
  - Provide a course of action
  - Provide for interoperability
- Baselines
  - Minimum level of security
  - System specific
  - TCSEC, ITSEC or Common Criteria
- Guidelines
  - Offers recommendations on applying standards and baselines
  - Prescribe security mechanisms
  - Not compulsory
- Procedures
  - Step-by-step how-to document
  - Usually software and hardware specific
  - Updated as systems evolve

Security Policies

- **Security Policies defines the scope of security needed, the assets that need protection, and the extent of solutions providing protection**

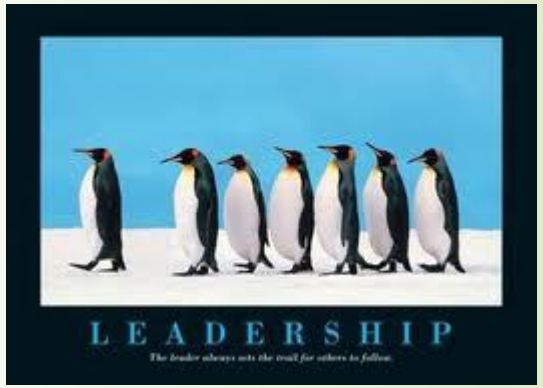
- Categories
  - Regulatory
    - Industrial or legal standards
  - Advisory
    - Most common
    - Acceptable behaviors
  - Informative

- Company goals
- Mission statements

- Types
  - Organizational
  - Issue-Specific
  - System-Specific

Business Continuity Planning (BCP) / Disaster Recovery Planning (DRP) Senior Leadership Support

- **Without it, plan will fail**
- **Senior management commitment is a must!**
- **Top-down approach**
  - **More cooperation at all levels for continuity planning**
- **Establish policies regarding requirements, roles, and responsibilities**
- **Establish budget / approve funding**



BCP/DRP Executive Management Support

- Support is required to:
  - Initiate the plan
  - Final approval of the plan
  - Demonstrate due care and due diligence and to be held liable under applicable laws and regulations

BCP/DRP Project Manager

- **Key point of contact for every person during a crisis**
- **Must be creditable and have the authority to make important, critical decisions**
- **Need not be technically endowed but have good business skills and be extremely competent**

BCP/DRP

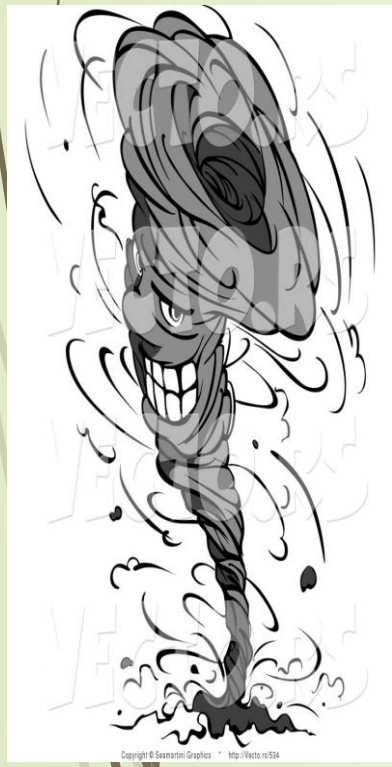
- The BCP focuses on the business as a whole (strategic) while the DRP is more information system centric (tactical)
- The DRP is a subset of the overall BCP
- The BCP protects the business before, during, and after a disruptive event
  - The DRP is a tactical method for immediately dealing with disruptions

Potential Loss Categories

- Risks to the corporation found in three areas:
  - Financial
    - Revenue Loss, Extra Expenses
    - Calculate financial risk
      - P * M = C

  - Reputational
    - Compromised Customer Service
    - Embarrassment/Loss of Confidence
  - Regulatory

Disasters or Disruptive Events



- Three Common Categories
  - Natural
    - Natural Disasters (Natural)
  - Human
    - Error and Omissions (Human)
    - Warfare, Terrorism, and Sabotage (Human)
    - Financially Motivated (Human)
    - Strikes (Human)
  - Environmental
    - Temperature and Humidity Failures (Environment)
    - Pandemics and disease (Environment)
  - Electrical (All types)
  - Personnel Shortages (All types)
  - Communication Failures (All types)

Developing a BCP/DRP

- Develop Contingency Planning Policy Statement
- Conduct the Business Impact Assessment (BIA)
- Identify Preventative Controls
- Develop Recovery Strategies
- Develop an IT Contingency Plan
- Plan Testing, Training and exercises
- Plan Maintenance

Business Impact Assessment

- Determines impacts associated with possible threats to information systems
- Assist in determining components which support business processes
- Provides the basis for the levels and types of protection required
- Determine metrics:
  - Recovery Time Objectives (RTO)
  - Recovery Point Objective (RPO)
  - Maximum Tolerable Downtime (MTD)
- Critical activities of a BIA:
  - Criticality prioritization
  - Downtime estimation
  - Resource requirements

Business Impact Assessment

Business Impact Assessment

- **Sample BIA Form**

Functional Name	Function Name	Mail Zone	Risk Code	Time before Impact	Customer Impact	Regulatory Impact	Financial Impact	Rating Total	Recovery Time Sensitivity Code	Alt. Site
			F = Financial C = Customer R = Regulatory	0 = week 2 or more 1 = week 1 5 = up to three days 10 = day 1 20 = 4 hours 40 = immediate	0 = none 1 = Low 3 = Med 5 = High	0 = none 1 = Low 3 = Med 5 = High	0 = none 1 = 0 to 10K 2 => 10K but < 100K 3 => 100K but < 500K 4 => 500K but < 1 Mil 5 => 1 Mil	Sum of 1 through 4		
Customer service	Call Center	Z 45	C & F	40	5	1	3	49	AAA	Surviving sites then Smith Road
Customer service	Customer account maint	Z 37	C & F	1	3	0	0	4	D	Work from Home
Customer service	Customer monetrary	Z 38	C & F & R	10	3	3	4	20	AAA	Smith Road

Components of the Enterprise Continuity Planning Process

- **Business Continuity Planning (BCP)**
- **Disaster Recovery Planning (DRP)**
- **Crisis Management Planning (CMP)**
- **Continuous Availability (CA)**
- **Incident Command System (ICS)**

Benefits to Continuity Planning

- Organizational analysis may identify potential efficiencies and costs savings
- New business opportunities
  - Advantage over other competitors
- Reduced insurance rates

Contingency Planning Policy Statement

- **Provides the authority and guidance necessary to develop the Contingency Plan**
- **The scope of the planning effort will define the:**
  - **Project resources needed**
  - **The timeline to complete it**
  - **The deliverables expected**

Critical State Assessment

- Determine the parts of the IT infrastructure that are critical
- Identifying critical assets requires communication between the users and planners
- Tool: Critical State and Asset List
  - Identify the asset, the user, the process affected and the impact

Continuity Planning Project Team (CPPT)

- Comprised of stakeholders within a company
- Focuses on identifying personnel needed to play key roles in the case of an emergency
- A key challenge is the manager/employee relationship
  - Many employees work under different managers for different projects. Identifying where they are used in an emergency situation is difficult

BCP/DCP Considerations

- Additionally a company should be aware of BCP of its:
  - Third party providers
  - Key suppliers
  - Business partners

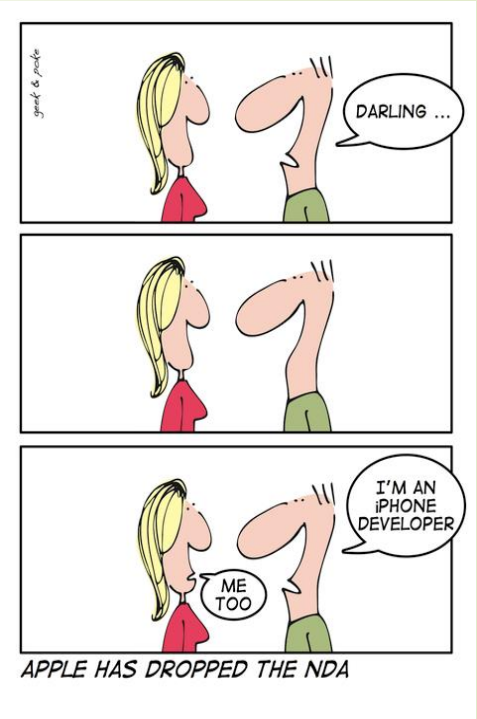
- When a company outsources information, transaction processing, and settlement activities, the company should review and understand service provider's BCP and ensure critical services can be restored within acceptable timeframes based upon the needs of the institution
- If possible it recommends the institution consider participating in their provider's testing process.

BCP/DRP Considerations - Regulations

- **NIST SP 800-34**
- **ISO/IEC 27031**
- **British Standard (BS) 25999**
- **Business Continuity Institute (BCI)**
- **Federal Financial Institutions Examination Council (FFIEC) BCP Booklet**
- **National Association of Security Dealers (NASD) Rule 3510**
- **NYSE Rule 446**
- **Electronic Funds Transfer Act**
- **Basel Committee**
- **HIPAA**
- **Sarbanes-Oxley Section 404**

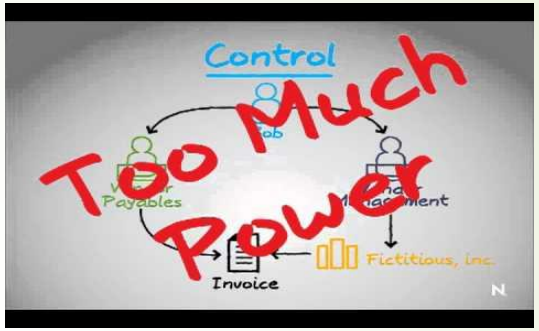
Employment Policies & Practices

- Screening
- Background Checks
- Employment agreement
  - Rules & restrictions
  - Security policy
  - Acceptable use
  - Job description
  - Violations & consequences
- Nondisclosure agreement (NDA)



Administrative Control Methods

- Separation of Responsibilities
- Principle of Least Privilege (POLP)
- Need to Know
- Job Rotation
- Mandatory Vacations
- Security Audits and Reviews
- Supervision
- IO Controls
- Antivirus Management



Employee Termination

- Employee Termination
  - Termination Policy
  - Private
  - Witness
  - Exit interview
  - Disable network access
  - Accompaniment while on premises

Vendor, Consultant, and Contractor Security

- **Non-direct employees may have access to areas that, as a result, pose a significant risk.**
- **3rd party personnel should be trained similar to the training a regular employee receives**
- **3rd party rules of access should be developed**
- **Background checks should be considered**
- **Vendors with access to multiple sites may pose a risk by how they standardize their credentials or access**

Risk Management

- Risk Management
  - Involves reducing risks to an acceptable level
- Risk
  - Possibility of damage, destruction, disclosure
- Risk Analysis
  - Likelihood of occurrence
  - Cost of occurrence
  - Cost of countermeasures
  - Cost/Benefit report

Risk Terminology

- Asset
- Asset Valuation
- Threats
- Threat Agent
- Vulnerability
- Exposure
- Risk
- Safeguards (Countermeasure)
- Attack
- Breach

Risk Lifecycle

Audit Frameworks for Compliance

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Information Technology Infrastructure Library (ITIL)
- Control Objectives for Information and Related Technology (COBIT)
- ISO 27002 aka ISO 17799/BS7799-2 (ISO 27001)

Risk Assessment Methodologies

- NIST SP 800-30r1, 800-39, and 800-66r1
- Central Communication and Telecommunication Agency (CCTA) Risk Analysis and Management Method (CRAMM)
- Failure Modes and Effects Analysis (FMEA)
- Facilitated Risk Analysis Process (FRAP)
- Operationally Critical Threat Asset & Vulnerability Evaluation (OCTAVE)
- Security Officers Management and Analysis Project (SOMAP)
- Spanning Tree Analysis
- Value at Risk (VAR)

Qualitative Risk Analysis

- **Techniques & Methods**

Brainstorming	Delphi technique
Storyboarding	Focus groups
Surveys/Questionnaires	Checklists
One-on-one meetings	Interviews

(Probability vs. Impact: semiquantitative)

Quantitative Risk Analysis

- Assign a specific dollar value
- Valuation
  - Purchase cost
  - Market valuation
  - Intellectual property
  - Replacement cost
  - Liability of asset lost
  - Usefulness

Formulas for Risk

Total Risk

- **Asset value (AV) x Threats x Vulnerabilities = Total Risk**

Single Loss Expectancy (SLE)

- **AV x EF = SLE**

Annual Loss Expectancy (ALE)

- **SLE x Annualized Rate of Occurrence (ARO) = ALE**

Return on Investment

- **ALE (before SG) – ALE (after SG) – Annual cost of SG = ROI**

Financial Risk

- **Probability x Magnitude = Cost of Prevention**

Annual Loss Expectancy (ALE) Example

The information and infrastructure residing in a data center in Virginia is valued at $1M. Tornados are a threat, but statistically occur once every 10 years. If a tornado hit, the destruction would reduce the value of the facility by 90%.

AV = $1M **EF = 90%** **ARO = 1/10**

SLE = AV * EF ($1M * .90) _____

ALE = SLE * ARO

ALE = ($1,000,000 * .90) * (1 / 10) = $90,000

Annual Loss Expectancy (ALE) Example

With an Annualized Loss Expectancy of $90,000 …

Would it be cost effective to rent a facility for $120,000/year for a redundant hot-site?

OR

Co-locate servers at a shared facility for $60,000/year in case of disaster?

Threat / Risk Calculations

- After Safeguards
  - Calculate new ALE for asset
  - Requires new EF & ARO
- Financially equitable?
  - ALE(before sg) – ALE(after sg) – Annual cost of safeguard = Value of safeguard
- Other factors
  - Legal Responsibility
  - Due Care
  - PR

Threat Sources

- Hacker gaining access to confidential information
- Virus infection
- Processing errors / buffer overflows
- Coding / programming errors
- User errors causing a system malfunction
- Privilege abuse
- Natural disasters that cause damage or injury
- Terrorism that causes injury or destroys systems
- Energy anomalies
- Theft

Risk Analysis

- Allows upper management decision making
- Cost/benefit analysis
- Identifies risk
- Quantifies the impact of threats
- Appraises the value of assets
- Annual cost of safeguard should be less than expected annual cost of asset loss

Risk Analysis Matrix

LIKELIHOOD OF OCCURRENCE	HAZARD SEVERITY				
	Negligible (1)	Slight (2)	Moderate (3)	High (4)	Very high (5)
Very Unlikely (A)	LOW	LOW	LOW	LOW	MEDIUM
Unlikely (B)	LOW	LOW	LOW	MEDIUM	MEDIUM
Possible (C)	LOW	LOW	MEDIUM	MEDIUM	HIGH
Likely (D)	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Very Likely (E)	LOW	MEDIUM	HIGH	HIGH	HIGH

Handling Risk

- Responses to Risk
  - Reduce
  - Assign
  - Accept
  - Avoid
  - Reject
- Good candidate for risk acceptance:
  - Low-likelihood
  - Low consequences
- Can not accept risk
  - High risk
  - Risk prohibited by law or regulation
  - Risk to life or safety
  - Where accepting the risk is not an option

Access Control Categories

- Three Categories of Access Control:
  - Administrative / Operational controls
    - Defines roles, responsibilities, policies, and administrative functions
  - Physical Controls
    - Non-technical environment, such as locks, fire management, gates, and guards
  - Technical / Logical Controls
    - Electronic controls, where controls are applied and validated and information on the state of the environment is produced

Access Control Types

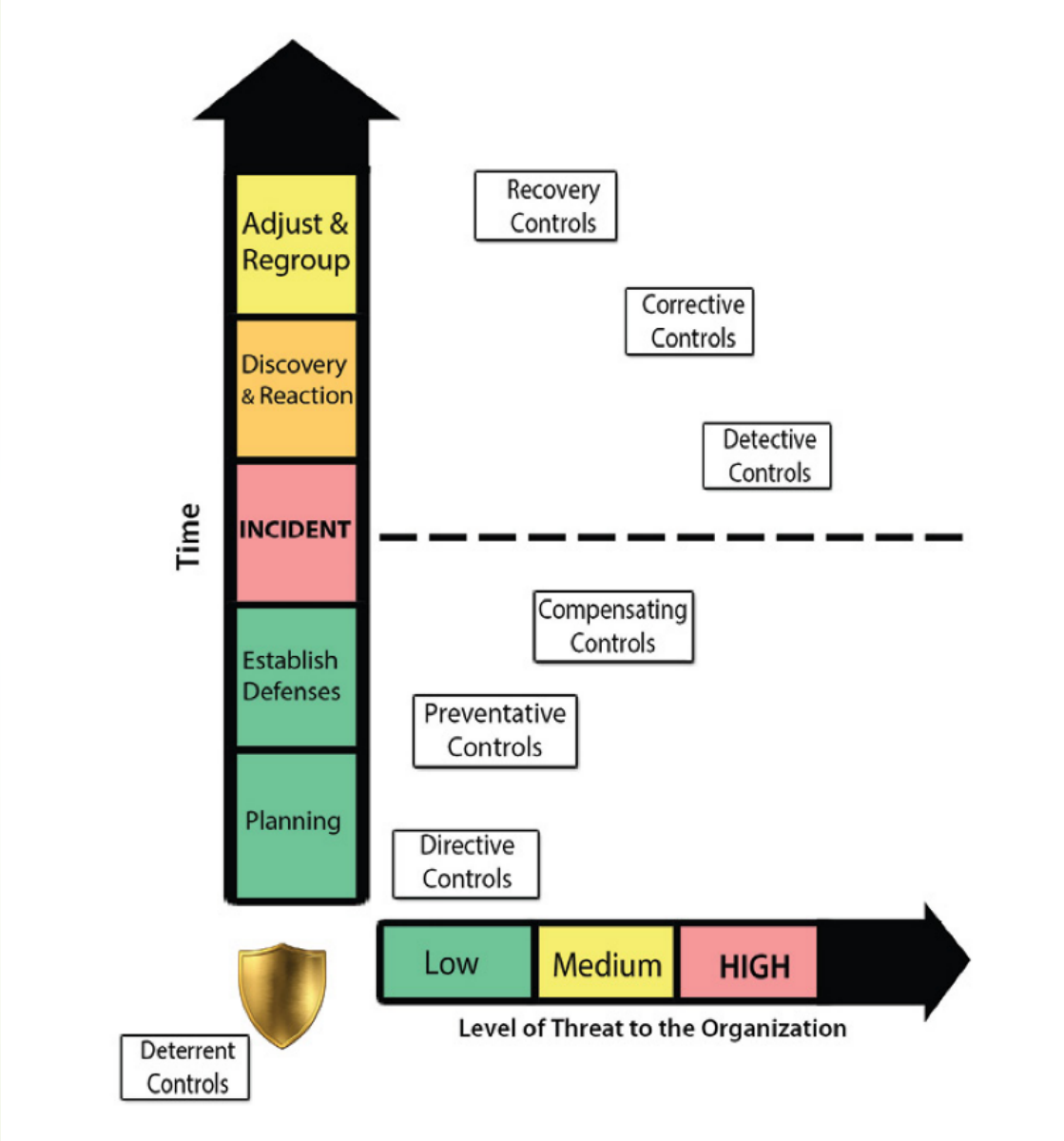
- Preventive – Stop unwanted / unauthorized activity
- Deterrent – Discourage a potential attacker
- Detective – Identify an incident's activities
- Corrective – Fix systems after an incident
- Recovery – Restores resources and capabilities
- Directive – Controls put in place due to regulation or environmental requirement
- Compensating – Provide alternatives to other controls (security policy, personnel supervision)

Access Control Examples by Category and Type

- Use the concept of "defense in depth" by layering levels of access controls.

	Deterrent	Preventive	Detective	Corrective	Recovery	Compensating
Administrative	Policy	User Registration Procedures	Review Violation Report	Termination	Disaster Recovery Plan	Supervision, Job Rotation
Technical	Warning Banner	Password Based Login	Logs, IDS	Unplug, Isolate, Terminate Connection	Tape backup	Logging, CCTV, Keystroke monitoring
Physical	Beware of Dog Sign	Fence	Sentry, CCTV	Fire Extinguisher	Reconstruct, Rebuild	Layered Defense

Continuum of Controls Relative to a Time Line



Vulnerability Testing

- Evaluating a system or network against a predefined list of vulnerabilities
  - System misconfiguration
  - Outdated software
  - Missing patches

- Popular testing tools:
  - Nessus
  - OpenVAS
  - Retina
  - SATAN/SAINT

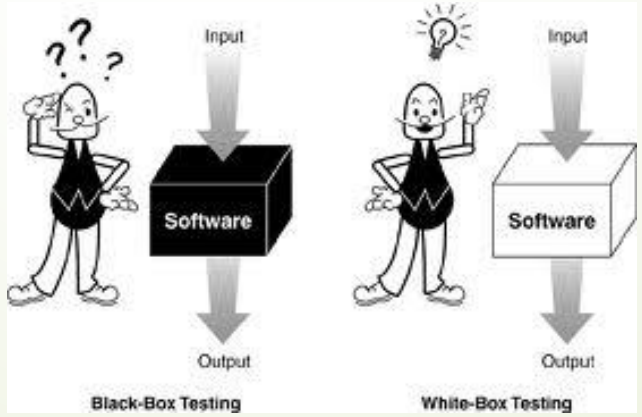
Penetration Testing

- Primary goal is to simulate an attack to evaluate the risk characteristics of an environment
- Secondary goal is to test the organizational incident response
- Can be employed against anything; usually focus is Internet system and services

Penetration Testing Strategies

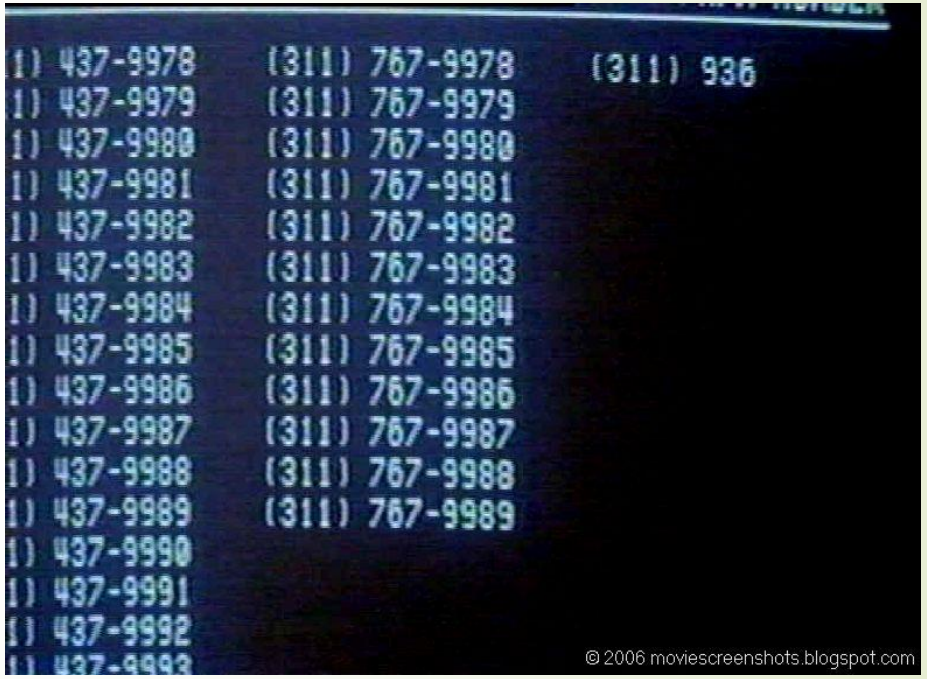
- External Testing
- Internal Testing
- Blind Testing
- Double Blind Testing
- Targeted Testing

- 3 basic categories of penetration test:
  - Zero knowledge (AKA black box or closed)
  - Partial Knowledge
  - Full Knowledge (white/crystal box)



Types of Testing

- Application testing
- Denial-of-service testing
- War dialing
- Wireless network testing
- Social Engineering
- PBX and IP phone testing



Penetration Test Methodology

- Reconnaissance/Discovery
  - Identify and document information about the target
- Enumeration
  - Gain more information with intrusive methods
- Vulnerability Analysis
  - Map the target environment profile to known vulnerabilities
- Execution

  Attempt to gain user and privileged access
- Document Findings
  - Document the results of the test

Tangible/Intangible Assets Valuation

- Tangible
  - Physical presence
  - Valued on cost – depreciation
  - Must be aware of replacement cost

- Intangible
  - Not physical (trademarks, patents, copyrights, brand recognition, etc.)
  - Definite intangible
    - Definite expiration period
  - Indefinite intangible
    - Indefinite expiration period

Continuous Improvement

- Plan-Do-Check-Act (PDCA) cycle AKA: Deming Cycle/Shewhart Cycle
  - Plan: identify an opportunity and plan for change
  - Do: Implement the change on a small scale
  - Check: analyze the results of the change
  - Act: If successful implement on a wider scale; if the change did not work, begin the cycle again

- Other methods:
  - Six Sigma
  - Lean
  - Total Quality Management

Enterprise Risk Management

- Encompasses:
  - Aligning Risk Appetite and Strategy
  - Enhancing Risk Response Decisions
  - Reducing Operational Surprises and Losses
  - Identifying and Managing Multiple and Cross-Enterprise Risks
  - Seizing Opportunities
  - Improving Deployment of Capital

Enterprise Risk Management

- Definition:
  - A process, ongoing and flowing through an entity
  - Effected by people at every level
  - Applied in a strategy setting
  - Applied across the enterprise, at every level
  - Designed to identify potential events that could effect the entity
  - Able to provide reasonable assurance to an entity's management and board of directors
  - Geared to achievement of objectives in one or more separate but overlapping categories

Achievement of Objectives

- Four categories
  - Strategic: high-level goals, supporting the mission
  - Operations: effective and efficient use of resources
  - Reporting: reliability of reporting
  - Compliance: compliance with applicable laws and regulations

Components of Enterprise Risk Management

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

Risk Management Framework (RMF)

- Ensures that key risks are effectively identified and responded to in a manner that is appropriate to:
  - The nature of the risks faced by the organization
  - The organization's ability to accept and/or manage risks
  - The resources available to manage risks within the organization
  - The organization's culture

Risk Management Framework (RMF)

- The RISK IT Framework (ISACA)
- ISO 31000:2009 Risk Management
- Enterprise Risk Management – Integrated Framework (COSO)
- NIST SP 800-37r1 Risk Management Framework (RMF)

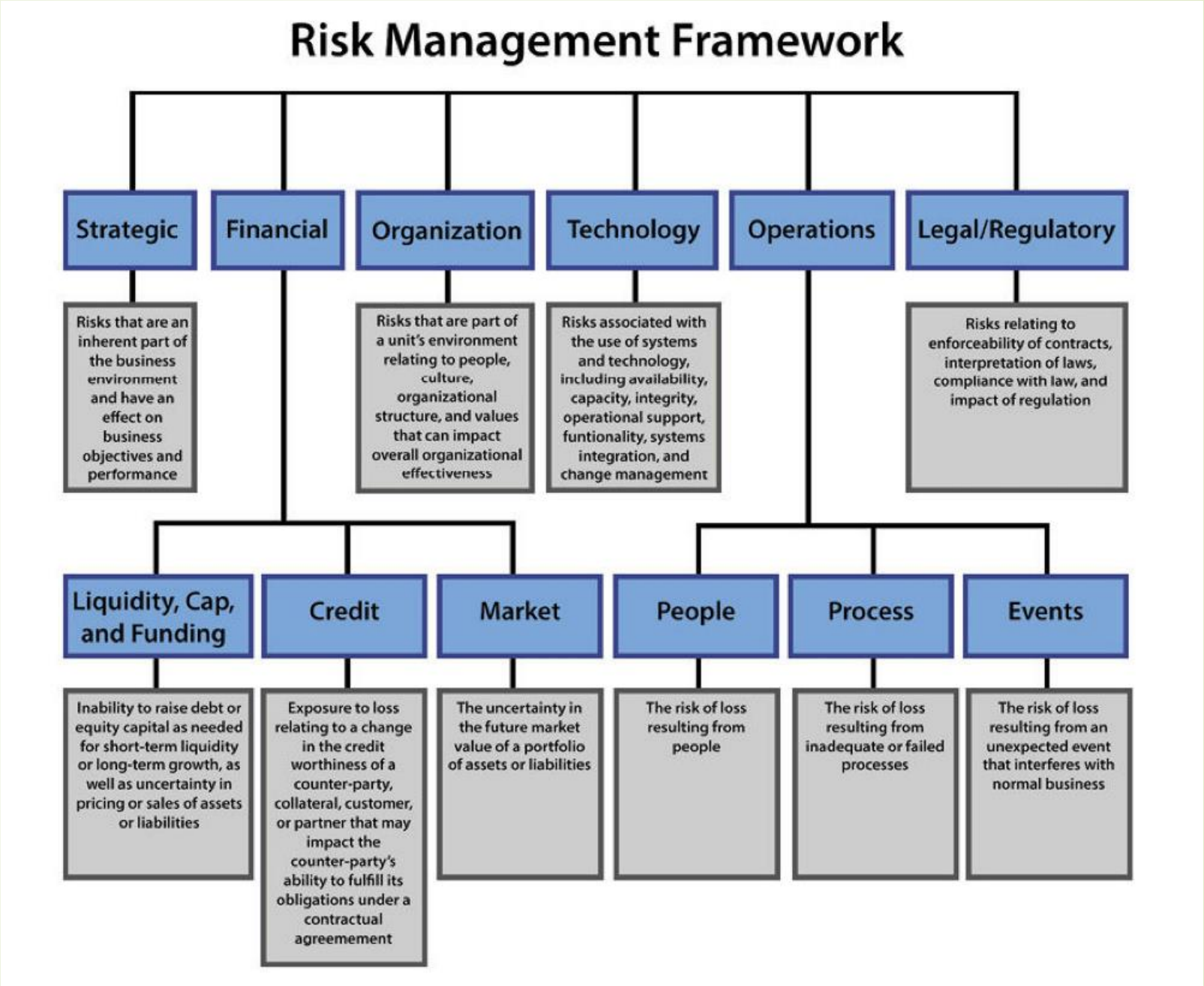
Risk Management Framework (RMF) Characteristics

- Promote near real-time risk management
- Encourage the use of automation to provide information to decision makers
- Integrate information security into the enterprise architecture and system development lifecycle
- Provide emphasis on the selection, implementation, assessment, and monitoring of security controls and the authorization of information systems
- Link risk management processes at the information level to risk management processes at the organizational level
- Establish responsibility and accountability for security controls

Risk Management Framework (RMF) Steps

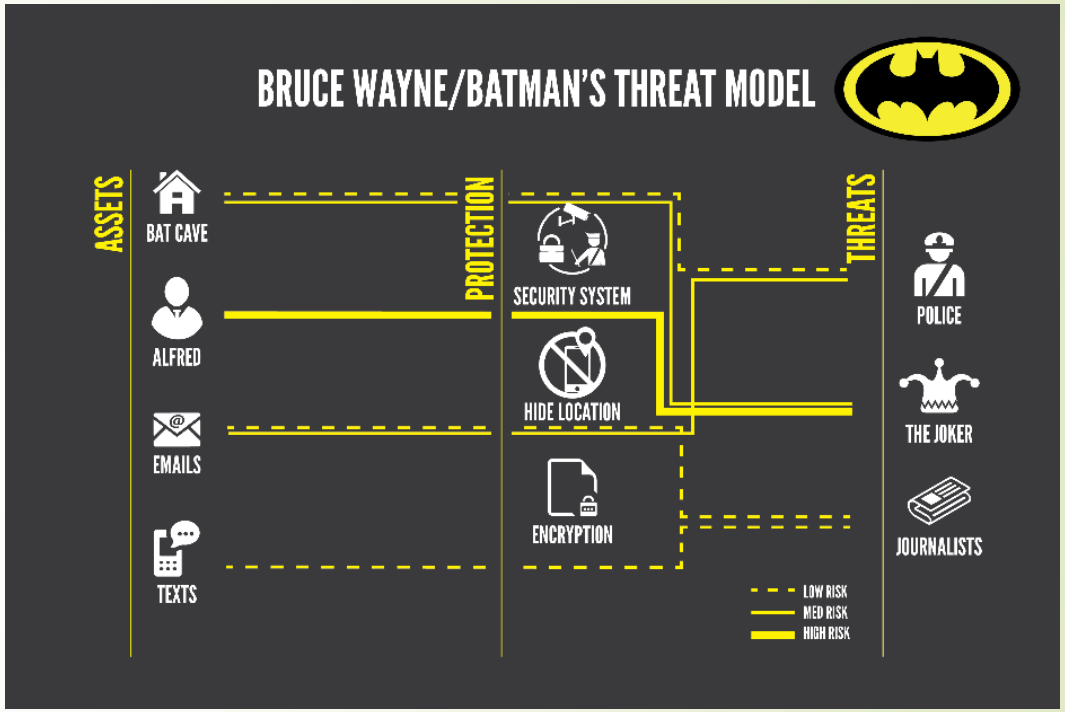
- Categorize the information system and information processed, stored and transmitted
- Select an initial set of baseline security controls
- Implement the security controls
- Assess the security controls
- Authorize information system operation based on acceptable risk
- Monitor the security controls on an ongoing basis

Risk Management Framework (RMF)



Threat Modeling

- Enables informed decision making
- Can produce a prioritized list of security improvements
- Part of the design phase of SDLC
- A procedure for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities and then defining countermeasures to prevent or mitigate the threat



Acquisitions Strategy and Practice

- Supply Chain
  - A tangible asset
  - Subject to disruption
  - Cyber related supply chain disruptions are rare
  - Large scale cyber events pose a potential threat as damaging as a natural disaster
  - Supply chain usually means the movement of physical assets
    - The concept needs to be expanded to include services and information
  - A purchase of products or services that have inadequate built-in security present a risk that persists throughout the lifecycle of the item

Comprehensive Enterprise Response to Cyber Risks

- Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
- Address cybersecurity through relevant training
- Develop common cybersecurity definitions for acquisitions
- Institute an acquisition cyber risk management strategy
- Include a requirement to purchase from Original Equipment Manufacturers (OEMs), their authorized resellers, or other "trusted" sources, whenever available, in appropriate acquisitions
- Increase the organizational accountability for cyber risk management

3rd Party Governance

- Cloud computing
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Utilize Service Level Agreements(SLA)
- Assurance only possible through inspection, review, and assessment (of 3rd party system documentation).
- Determine legal exposure of:
  - Outsourcing
  - Offshoring

Minimum Security and Service-Level Requirements

- **Statement of Requirements**
- **Service Level Requirements (SLR)**
- **Service Level Agreement (SLA)**
- **Service Level Report**

Security Awareness Training

- Goal - behavior modification
- Learning levels
  - Awareness
  - Training
  - Education
- Should cover a broad range of topics

Questions?

Practical Exercise

- **Quantitative Risk Analysis exercise**
- **Time allotted: 20 minutes**

Asset Security

(Protecting Security of Assets)

Domain Objectives

- Determine and Maintain Ownership
- Establish Handling Requirements
- Classify Information and Supporting Assets
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls

Good Data Management Practices

- Data policy that defines long term goals
- Clearly defined roles and responsibilities
- Data quality procedures at all stages of data management
- Documentation of data management practices
- Adherence to agreed upon data management practices
- Carefully planned and documented database specifications
- Defined procedures for updating
- Ongoing data audit
- Ongoing and evolving data security approach
- Clear statements of criteria for data access
- Clear and documented published data that is available to users

Data Policy

- Issues to be considered:
  - Cost
  - Ownership and Custodianship
  - Privacy
  - Liability
  - Sensitivity
  - Existing law and policy requirements
  - Policy and process

Data Management Roles and Responsibilities

- Created to:
  - Define roles associated with functions
  - Establish data ownership throughout all phases
  - Instill data accountability
  - Ensure that adequate and agreed upon data quality and metadata metrics are maintained on a continuous basis

Data Ownership

- Information owner responsibilities:
  - Determine impact of information on mission
  - Understand replacement cost of the information (if replaceable)
  - Determine who has a need for the information and under what circumstances
  - Know when the information is inaccurate or no longer needed

Data Custodianship

- Data custodian responsibilities:
  - Adherence to appropriate and relevant data policy and data ownership guidelines
  - Ensure accessibility to appropriate users
  - Fundamental data maintenance
    - Storage/archiving/backup
  - Data documentation (update)
  - Assurance of quality and validation of additions
    - Periodic audits (integrity)

Data Quality

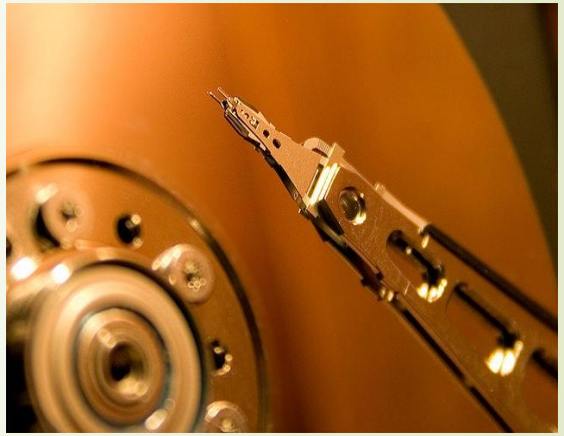
- Quality Control (QC): assessment of quality based on internal standards, processes, or procedures established to control quality
- Quality Assurance (QA): assessment of quality based on external standards used to review activities of quality control processes
- QA/QC mechanisms are designed to protect against data contamination
- Two fundamental types of errors:
  - Errors of commission
    - Data entry error or faulty equipment
  - Errors of omission
    - Insufficient documentation

Establish Handling Requirements

- **Media storing sensitive information requires physical and logical controls such as:**
  - **Labeling/Marking**
  - **Handling**
  - **Storage**
  - **Destruction/Sanitation**
  - **Retention**
  - **Data Remanence**

Data Remanence

- Data, once deleted, will remain until overwritten
- Residual data must be physically eliminated or it will run the risk of being recovered by unwanted parties.
  - Clearing (remove data in a way that it can not be reconstructed using normal techniques)
  - Purging (remove data in a way it can not be reconstructed by any known technique)
  - Degaussing (magnetic field)
  - Overwrite with 1s and 0s
  - Destruction
  - Encryption (delete SSD encryption key)



Destruction and Disposal

- Electronic files must be deleted in a manner that prohibits their retrieval by undoing the last action or restoring from a recycle bin
- Backup copies must be dealt with in the same manner as the original
- Data storage devices must be properly wiped prior to disposal

Information Classification

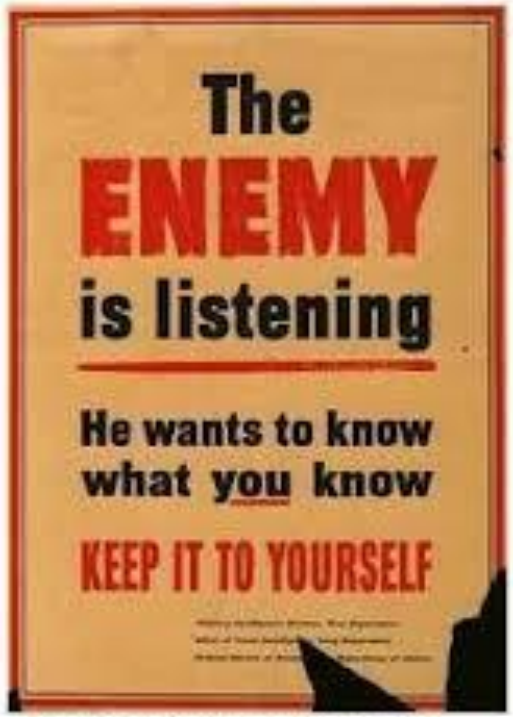


Image: American Merchant Marine at War

- The practice of evaluating the risk level of the organization's information to ensure that the information receives the appropriate level of protection

Data Classification

- Method to classify data by it's need for:
  - Secrecy
  - Sensitivity
  - Confidentiality
- Determines effort, money, & resources allocated to protect data
- Formalize & stratify the labeling process

Data Classification

	Level	Type	Result if Disclosed
Military	**Top Secret**	highest	grave danger
	Secret	restricted data	critical damage
	Confidential	between secret and SBU	serious damage
	SBU	private in nature	no significant damage
	Unclassified	lowest	no noticeable damage
Commercial	**Confidential**	highest; extremely sensitive	negative impact
	Private	personal in nature	significant negative impact
	Sensitive	more classified than public	negative impact
	Public	lowest	no serious impact

Proprietary data - form of confidential; drastic effects to competitive edge

Asset Management

- Includes disciplines such as:
  - Inventory Management
  - Configuration Management
  - IT Asset Management (ITAM)
  - Configuration Management Database (CMDB)

Asset Management

- **Assets that require protection:**
  - **Software**
  - **Equipment**
  - **Personal Information**

Basic Steps for Creating a Retention Policy

- Evaluate requirements, obligations and needs
- Classify types of records
- Determine retention periods and destruction practices
- Draft and justify record retention policy
- Train staff
- Audit retention and destruction practices
- Periodically review policy
- Document policy, implementation, training , and audits

Record Retention Policy

- Only keep data as long as it is required
  - Some retention is based on industry standards or compliance requirements
- Keep accurate records as to location and type of records stored
- Create a retention policy that addresses the differing types of records and their retention requirements
  - Do not apply the same retention requirements for all types of data

Data Security Controls

- Security mechanisms for:
  - Data in Storage
  - Data in Use
  - Data in Transit
    - Must address protection in wired and wireless networks
- Addresses
  - Data removal
  - Data destruction

Baselines

- Minimum level of security that each system must meet
- Establishes a common foundational secure state upon which additional and more stringent security measures can be built
- Benefits:
  - Only a minimum amount of resources are needed for risk management and management for each safeguard implemented
  - Offers cost-effective solution

Fundamental Principles of Information Security

- **Maintain the three overall objectives (confidentiality, integrity, and availability)**
- **Prevent, detect, respond, and recover**
- **Protect data in transit, storage, and while being processed**
- **External systems are assumed to be insecure**
- **Critical information systems need to be resilient to withstand major disruptive events**
- **Maintain auditability and accountability**

Scoping and Tailoring

- Scoping
  - Scoping guidance provides an enterprise with specific terms and conditions on the applicability and implementation of security controls
- Tailoring
  - Scoping the assessment procedures to more closely match the characteristics of the information system and its operating environment

Questions?

Security Engineering

(Engineering and Management of Security)

Domain Objectives

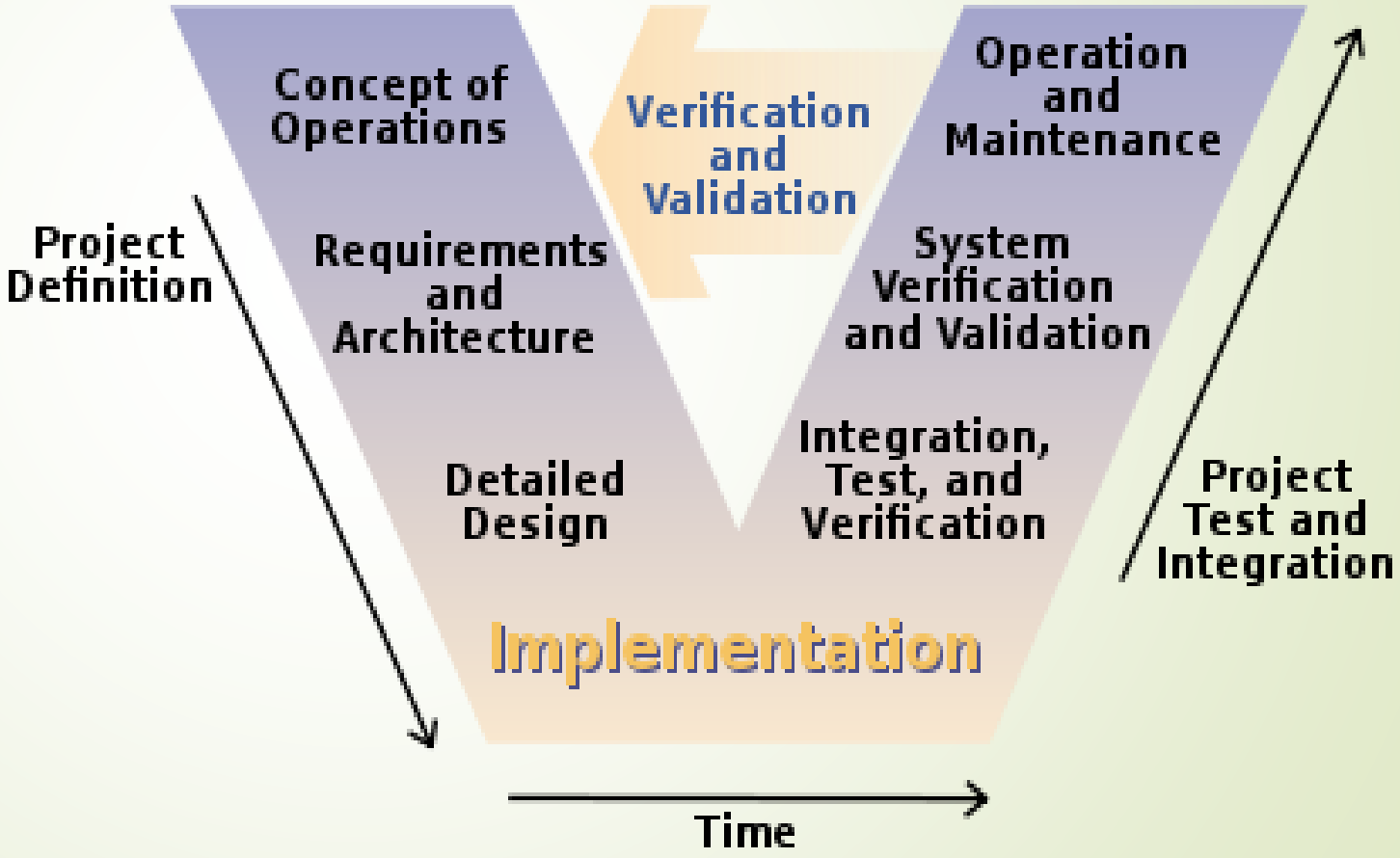
- **Understand the engineering lifecycle and apply security design principles**
- **Understand the fundamental concepts of security models**
- **Select controls and countermeasures based upon information systems security standards**
- **Understand the security capabilities of information systems**

Domain Objectives

- Assess and mitigate the vulnerabilities of:
  - Security architectures, designs, and solution elements
  - Web-based systems
  - Mobile systems
  - Embedded devices and cyber-physical systems
- Apply cryptography
- Apply secure principles to site and facility design
- Design and implement facility security

Engineering Lifecycle

- The V-Model



System Life Cycle Planning Phases

- Based on NIST SP 800-27 Rev A
  - Initiation
  - Development/Acquisition
  - Implementation
  - Operation/maintenance
  - Disposal

NIST SP 800-27 Rev A IT Security Principles (33)

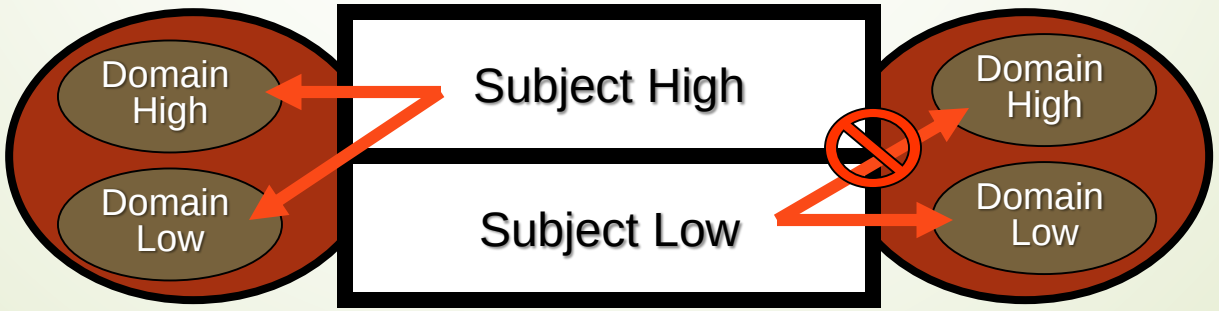
- Categories:
  - Security Foundation (principles 1-4)
  - Risk Based (principles 5-11)
  - Ease of Use (principles 12-15)
  - Increase Resilience (principles 16-23)
  - Reduce Vulnerabilities (principles 14-29)
  - Design with Network in Mind (principles 30-33)

Security Architecture Characteristics

- Has its own discrete security methodology
- Composes its own discrete views and viewpoints
- Addresses non-normative flows
- Introduces its own non-normative flows
- Introduces unique single-purpose components in the design
- Calls for its own unique set of skills and competencies of the enterprise and IT architects

Security Domains

- Trust between resources and services in realms that share a single security policy and management
- A concept where the principle of separation protects each resource and each domain
- An active directory domain or Kerberos Realm is an example of a security domain



Open / Closed Systems

- Open
  - Built open industrial standards
  - Interoperability between varying products from different vendors
- Closed
  - Closed systems are proprietary
  - Traditionally lack interoperability
  - Generally considered to be more secure

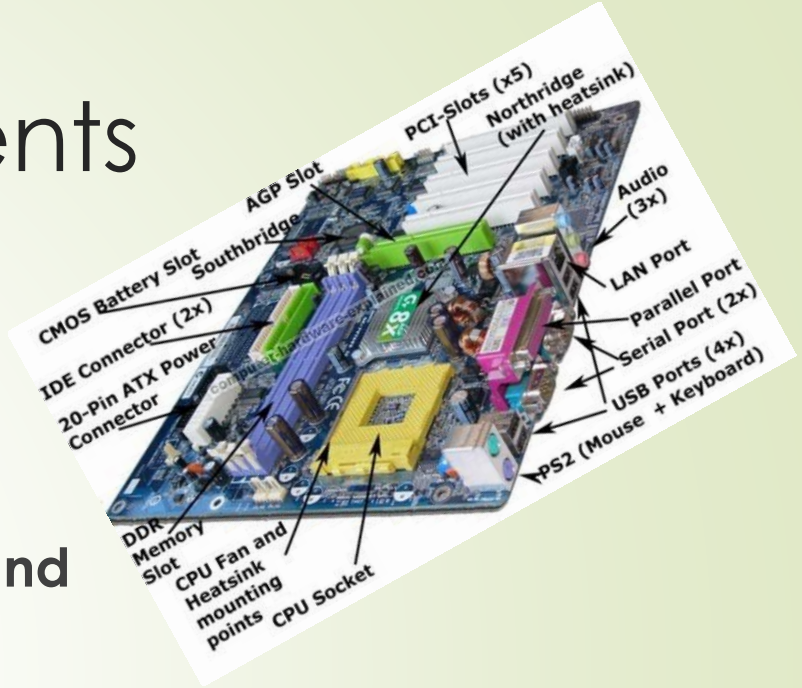
ISO/IEC 21827:2008

- The Systems Security Engineering – Capability Maturity Model (SSE-CMM)
- Is a secure development lifecycle framework
- Describes essential characteristics that must exist to ensure good security engineering
- Covers practices generally used in industry
- Provides a standard metric for security engineering practices

Common System Components

- **Processors – are the brains of a computer that performs calculations while solving problems and performing system tasks**
- **Storage devices – provide long and short term storage of information**
- **Peripherals (I/O) – are devices that either input or receive data**
- **Operating System (OS) – binds all of the components together and provides the interface for applications, utilities, and the end-user**

Additional System Components



- Buses
  - Northbridge (MCH)
  - Southbridge (ICH)
- Arithmetic Logic Unit
  - Math calculations
- Registers (base = start; limit = length)
  - Storage
- Control Unit
  - Synchronization and fetches
  - FDX (fetch, decode, execute, write)
  - Pipelining (combining different instructions during the FDX process)

Enterprise Security Architecture (ESA)

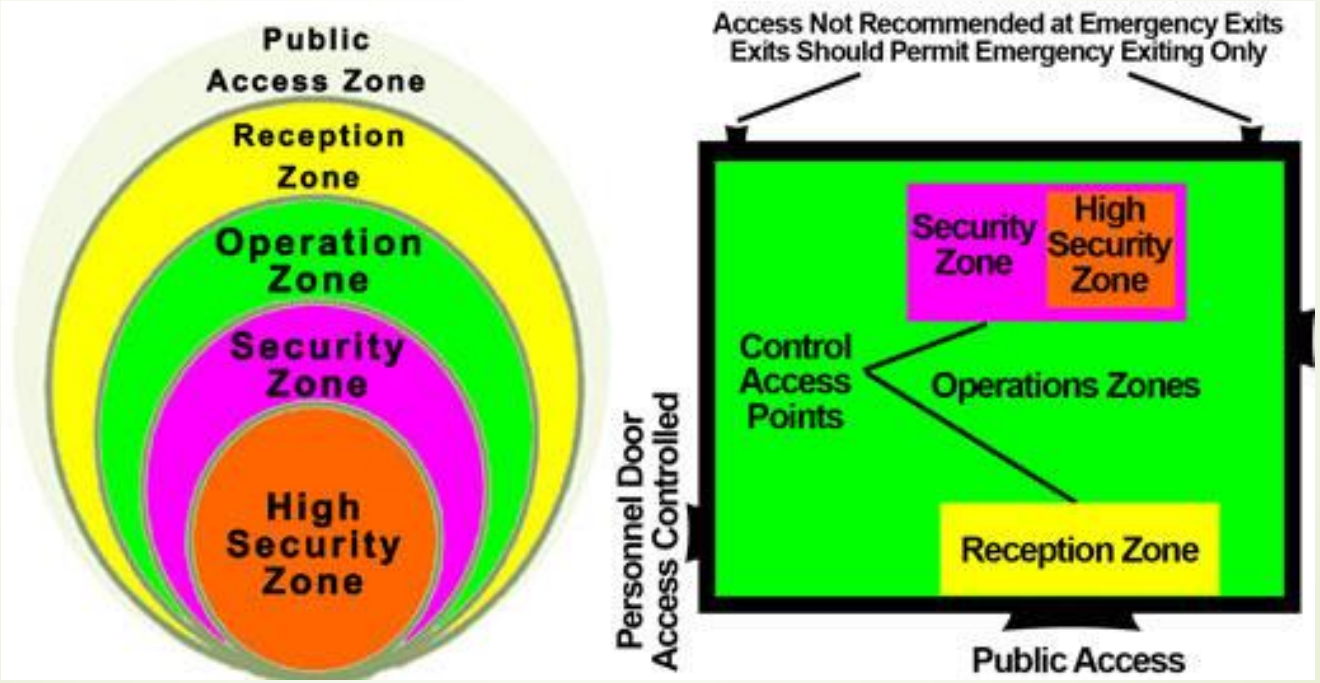
- **Implements the building blocks of information security infrastructure across the entire organization**
- **Focuses on strategic design for security services that can be leveraged across multiple applications, systems or processes**
- **Focused on long-term strategy**
- **Primary purpose: to establish the priorities for security services development and provide that input into information security program planning**

Common Security Services

- **Building blocks for ESA:**
  - **Boundary Control Services**
  - **Access Control Services**
  - **Integrity Services**
  - **Cryptographic Services**
  - **Audit and Monitoring Services**

Security Zone

- **An area or grouping within which a defined set of security policies and measures are applied to achieve a specific level of security**



Common Architecture Frameworks

- An architecture framework is a tool which can be used for developing a broad range of different architectures. It describes a method for designing an information system in terms of a set of building blocks, and for showing how the building blocks fit together. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.

- Common Architecture Frameworks:
  - Zachman Framework
  - Sherwood Applied Business Security Architecture (SABSA) Framework
  - The Open Group Architecture Framework (TOGAF)
  - IT Infrastructure Library (ITIL)

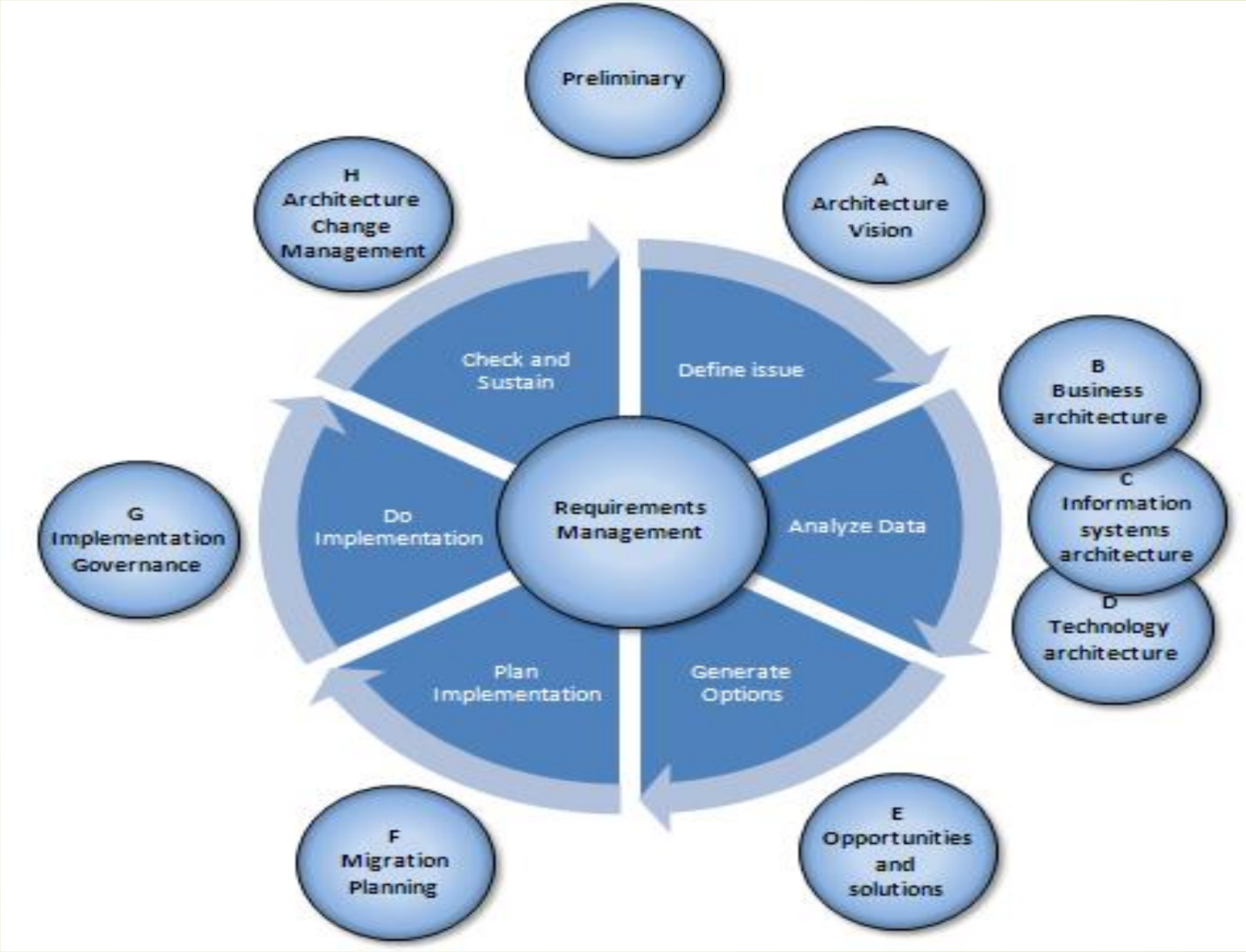
Zachman Framework

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Planner						
Owner						
Designer						
Builder						
Programmer						
User						

The SABSA matrix

SABSA	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

The Open Group Architecture Framework (TOGAF)



IT Infrastructure Library (ITIL)

Security Modes

- Mode of operation which the DAA accredits an IS to operate; based on
  - Sensitivity of the information
  - Clearance levels of the data to be processed
    - Dedicated
    - System High
    - Compartmented or Partitioned
    - Multilevel Security
  - Processing Types
    - Single State system
    - Multistate system

Security Modes Requirements

	Dedicated	System High	Compartmented	Multimode
Nondisclosure Agreement	Yes	Yes	Yes	Yes
Clearance	All	All	All	Some
Formal Access	All	All	Some	Some
Need To Know	All	Some	Some	Some

Security Models

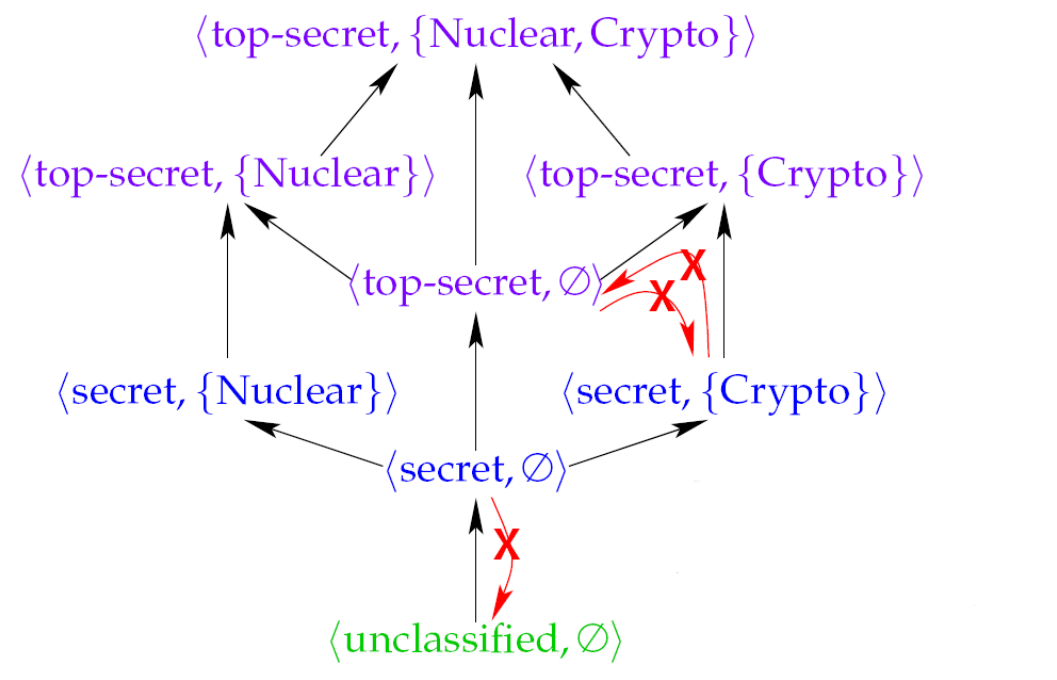
- Designing and building trusted computer systems
- Define allowed interactions between subjects and objects at a particular moment in time
- Will it support confidentiality or integrity?

State Machine Models

- Based on Finite State Model (FSM)
  - Always in a secure state
- States and transitions
- Security policy
- Basis for other models

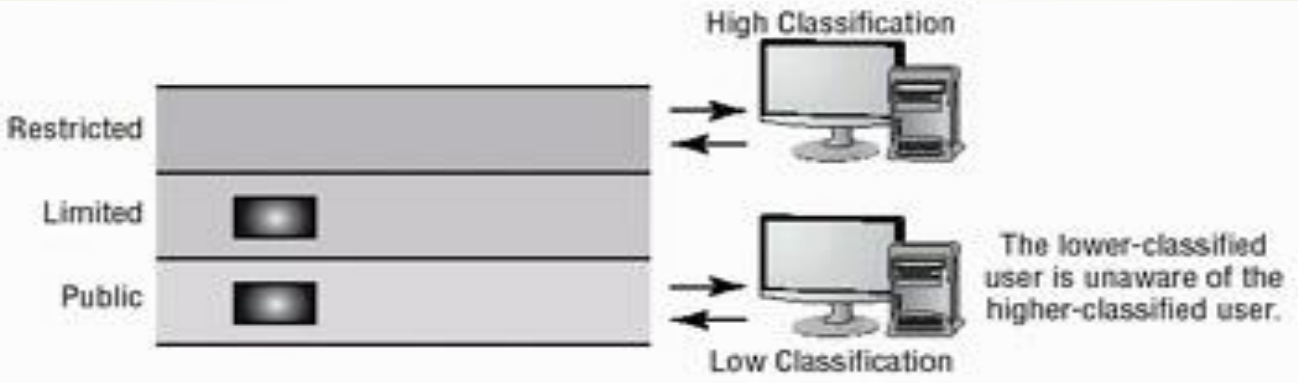
Multi-Level Lattice Models

- Zones of security (compartmentalization)
  - One way information flow
- Subjects are assigned security clearances
- Objects are assigned security labels



Non-interference Models

- Preventing high-level actions from being examined by low-level users
  - Information leakage
    - Inference attack (indirect covert channel)
  - Requires complete separation between security levels



Matrix Based Models

- Focus on one to one relationship between subject and object
- Access control matrix
- Typical access methods:
  - Read
  - Write
  - Edit
  - Delete

Access Control Matrix

Access Control Matrix

	Subject	File 1	File 2	File 3	File 4
	Larry	Read	Read, write	Read	Read, write
Capability	Curly	Full control	No access	Full control	Read
	Mo	Read, write	No access	Read	Full control
	Bob	Full control	Full control	No access	No access
				ACL	

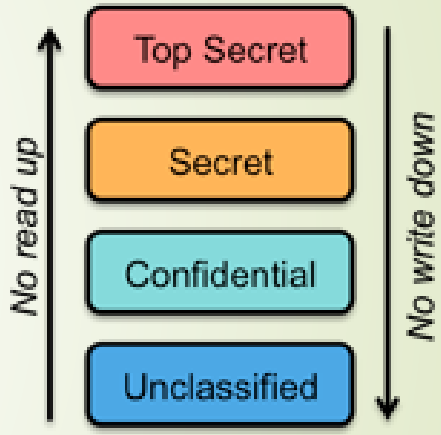
Capability = row in matrix
ACL = column in matrix

Information Flow Models

- State machine models that focus on the flow of information
  - Biba and Bell-LaPadula
  - Lattice based: one way flow
- Goal is to prevent covert channels

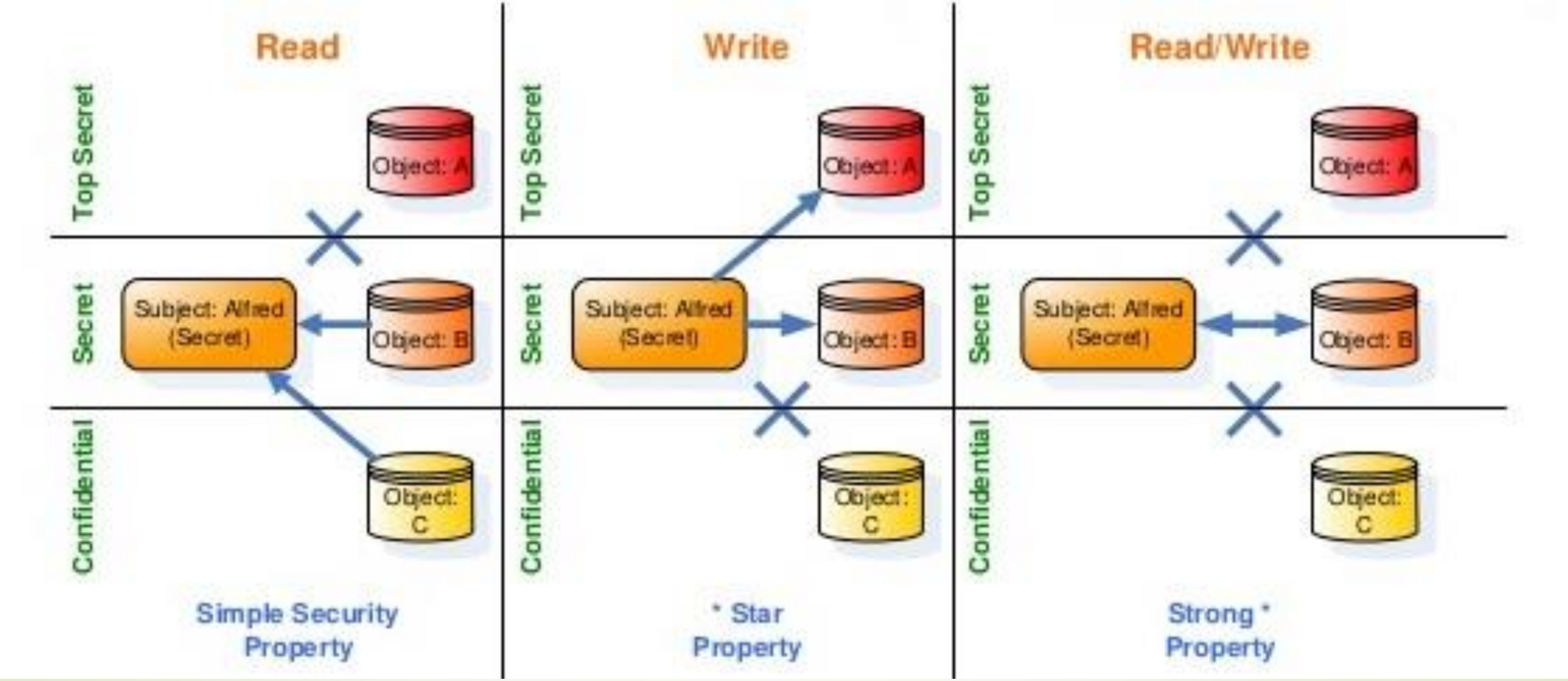
Bell-LaPadula Model

- Developed from the DoD multilevel security policy
  - Security labels
  - Need-to-know
  - First mathematical model of a multilevel security policy
- Blend of general security models
  - Information flow and state machine
  - Mandatory access controls and lattice model
- Simple Security Property: no read up
- * Security Property: no write down



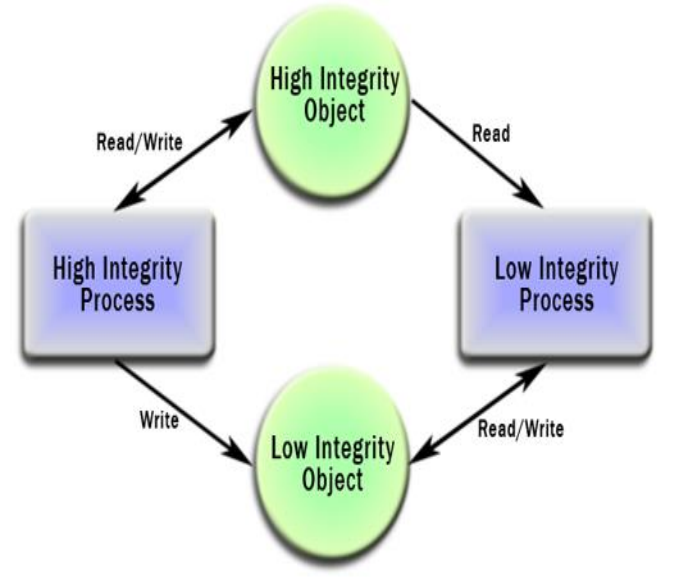
Confidential cannot read Secret
Confidential cannot write Unclassified

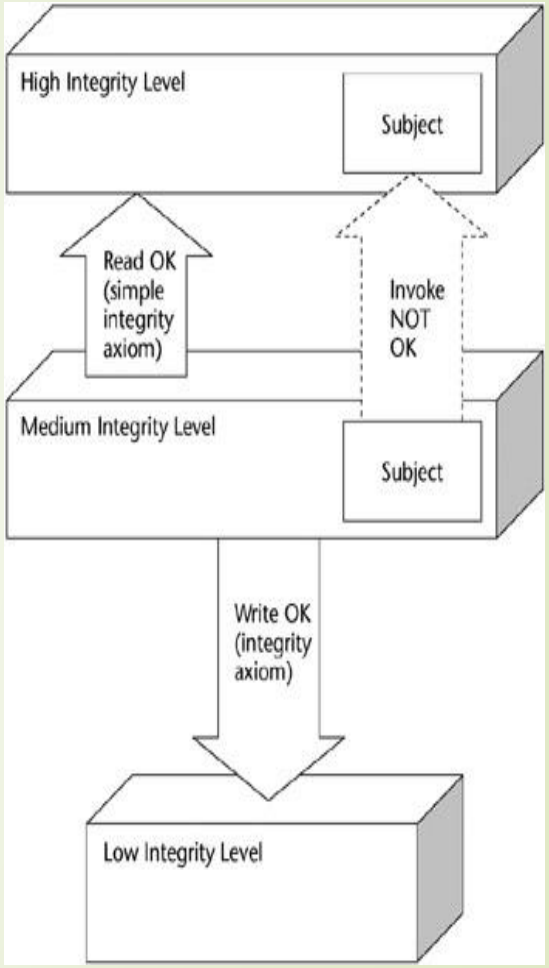
Bell-LaPadula Model



Biba Security Model

- Blend of general security models
  - Information flow and state machine
  - Concerned about the contamination of data
  - Mandatory access controls and lattice model
- Simple Integrity Axiom: no read down
- * Integrity Axiom: no write up





Clark-Wilson Model

- Focuses on integrity
  - Constrained data items (CDI) and Transformation Procedures (TP)
- Uses a subject/program/object relationship
  - Objects are accessed only through programs
  - Maintains internal/external consistency
- Separation of duties
  - Critical functions are broken up among multiple subjects
  - Prevents authorized subjects from making improper modifications to objects

Rule	Description
C1	IVPs must ensure that CDIs are valid
C2	TPs on CDIs must result in a valid CDI
C3	Separation of Privilege & least privilege
C4	TPs must be logged
C5	TPs on UDIs must result in a valid CDI
E1	Only certified TPs can operate on CDIs
E2	Users must only access CDIs through TPs for which they are authorised
E3	Users must be authenticated
E4	Only administrator can specify TP authorisations (i.e. MAC)

Lipner Model

- Combines elements of Bell LaPadula and Biba together with job functions or roles in order to protect confidentiality and integrity
- Two methods for implementing integrity
- One uses Bell-LaPadula confidentiality model
  - One uses both Bell-LaPadula and Biba integrity model together
  - Both methods assign security levels and functional categories to subjects and objects

Brewer and Nash Model

- AKA: "Chinese Wall"
- Goal is to prevent conflicts of interest
  - Information flow model
  - Subject is prevented from access information of two competing clients
- Subject's access controls change dynamically based on previous activities

Graham-Denning Model

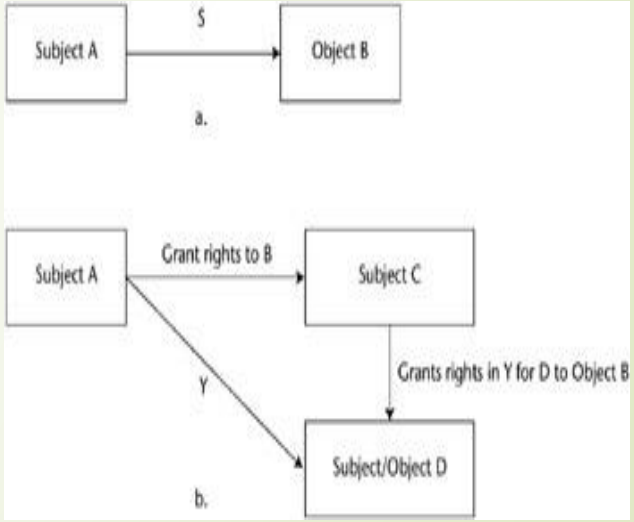
- Made up of 3 parts:
  - Subjects
  - Objects
  - A set of rights
- Subjects can manipulate objects or other subjects based upon their rights
- Eight Commands:
  - Create/Delete object
  - Create/Delete subject
  - Read/Grant/Delete/Transfer Access Right

Harrison-Ruzzo-Ullman Model

- Differs from Graham-Denning where it is concerned about a subject form gaining particular privileges.
- Subjects are prevented from accessing a particular program or sub routine that can execute a particular command where necessary (block SA)
- Composed of a set of generic rights and finite set of commands (create/destroy object; create/destroy subject; enter/delete right into access matrix)

Other Models

- Goguen-Mesequer Model (1982)
  - Domain separation; domain equals the objects a subject can access; capabilities table



- Sutherland Model (1986)
  - focuses on inference; based on state machine
- Take-Grant Model
  - Primary focus is on how subjects pass on their rights

Analyzing Requirements

- Establish the business requirements from key stakeholders and reviewers before proceeding with design work
- The following are needed to establish the goals and objectives for the design:
  - Principles
  - Guidelines
  - 2 main types of detailed requirements:
    - Functional Requirements
    - Nonfunctional Requirements

Security Policy

- Set of rules that dictates how information and resources is going to be managed
- Framework for the Security Architecture
- A multilevel security policy prevents information flow from a high security to a lower security level

Certification

- Comprehensive testing of a system and its safeguards
- Security evaluation criteria is compared to the testing results
  - Hardware, software, and configuration
  - Administrative, technical, and physical controls
  - Recertification is conducted at expiration or if system is changed

Accreditation

- Management compares system capabilities to the needs of the organization
- Formal declaration to accept system for specified period of time
- Changes require recertification
- Acceptance of “Residual Risk”
- Types:
  - Provisional
  - Full

Common Criteria

- Defacto standard for evaluating systems
- Globalized merger of the Information Technology Security Evaluation Criteria (ITSEC) and the Trusted Computer System Evaluation Criteria (TCSEC)
- Made an official standard by ISO
- Evaluation based on 7 Evaluation Assurance Levels (EALs)

Evaluation Assurance Levels

- EAL 1 Functionally Tested
- EAL 2 Structurally Tested
- EAL 3 Methodically tested and checked
- EAL 4 Methodically designed, tested, & reviewed
- EAL 5 Semiformally designed and tested
- EAL 6 Semiformally verified design and tested
- EAL 7 Formally verified design and tested

Comparing Security Evaluation Standards

TCSEC	ITSEC	CC	Designation
A1	F6+E6	EAL 7	Verified Security
B3	F5+E5	EAL 6	Security Domains
B2	F4+E4	EAL 5	Structured Security
B1	F3+E3	EAL 4	Security Labels
C2	F2+E2	EAL 3	Controlled Access
C1	F1+E1	EAL 2	Discretionary Security
D	E0	EAL 1	Minimal Security

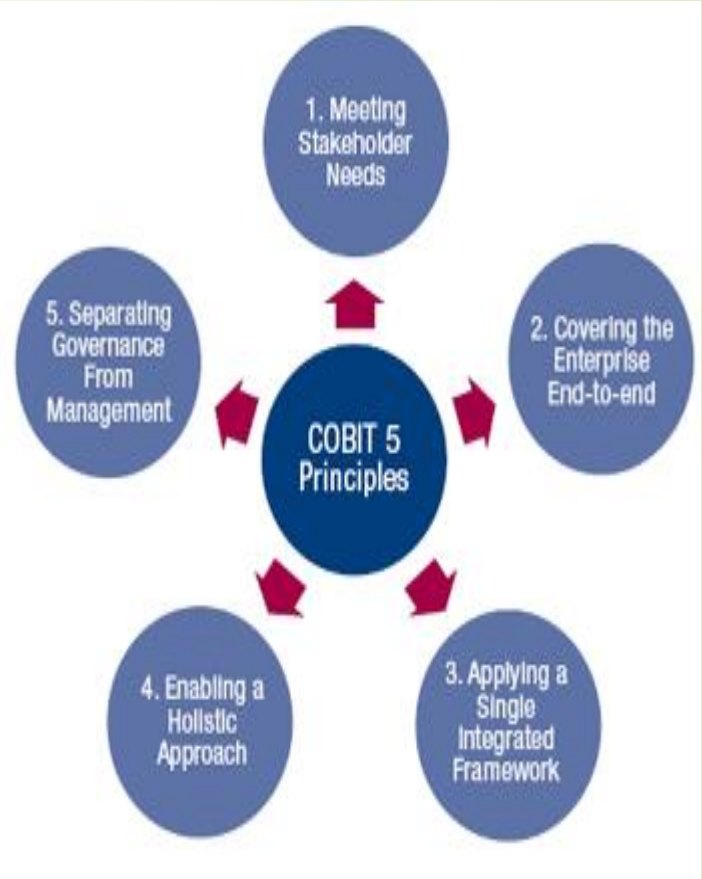
ISO/IEC 27001 & ISO/IEC 27002

- **ISO/IEC 27001: 2013**
  - **Focused on the standardization and certification of an organization's information security management system (ISMS)**
- **ISO/IEC 27002:2013**
  - **Code of practice for information security management**

(International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC))

Control Objects for Information and Related Technology (COBIT)

- Is a framework for IT management
- Provides a set of generally accepted processes to assist in maximizing the benefits derived using IT and developing appropriate IT governance
- It describes security controls as recommended by the IT auditing community
- Is the base minimum security services that every IT organization will need to implement



Payment Card Industry Data Security Standard (PCI DSS)

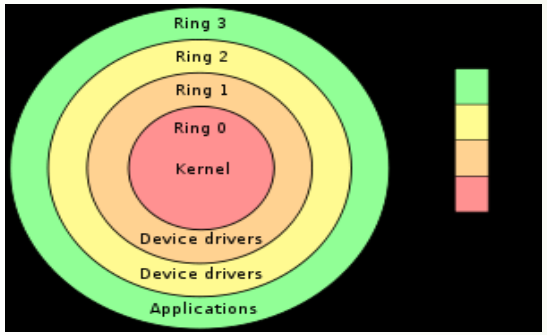
- Payment Card Industry Data Security Standard
- Created by payment card industry security standards council
- Provides the security architect with a framework of specifications to ensure the safe processing, storing and transmission of cardholder information
- Adopted by some states as a model for their state security requirements
- Has 6 core principles

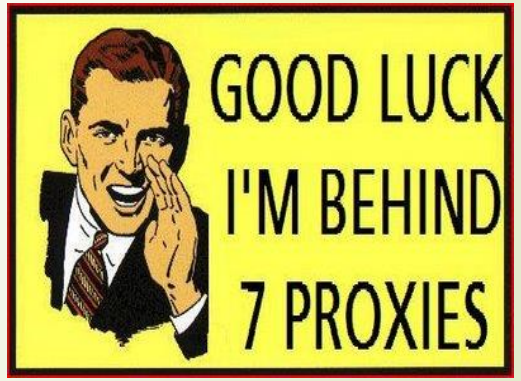
Security Capabilities of ISs

- Goal is to provide security without compromising the primary function of the system
- System protection techniques that may be applied across many layers of HW, firmware and SW:
  - Access Control Mechanisms
  - Secure Memory Management
  - Processor States
    - Two processor access modes:
      - User Mode: Application code runs in a non-privileged mode)
      - Kernel Mode: Processor has access to all system memory and all CPU instructions

Additional System Protection Techniques

- Layering
- Process Isolation
- Data Hiding
- Abstraction
- Auditing & Monitoring Controls





Additional System Protection Techniques

- Cryptographic Protection – using cryptography to protect sensitive system functions and data (i.e. using TPM)

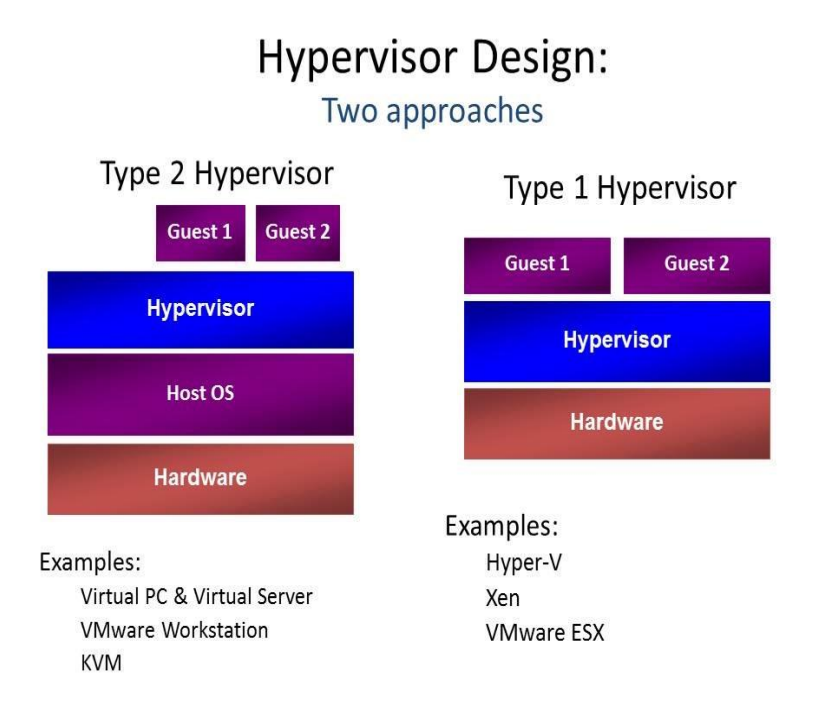
- Trusted Platform Module (TPM)
  - A microcontroller that stored keys, passwords and digital certificates
  - Typically affixed to the motherboard of a PC
  - More secure from external software attack and physical theft
  - Access to date and secrets in a platform could be denied, if the boot sequence is not as expected

Additional System Protection Techniques

- **Host Firewalls and Intrusion Prevention – used to protect individual hosts from attack**
  - **SW/HW Based Firewalls control traffic to and from a host**
  - **HIPS are used to validate network traffic directed at a host and block it from executing if its malicious in nature**

Additional System Protection Techniques

- Virtualization
  - Sandbox environment
  - Limited access to hardware resource
  - Quick deployment and removal
  - Two Methods:
    - Type 1
    - Type 2

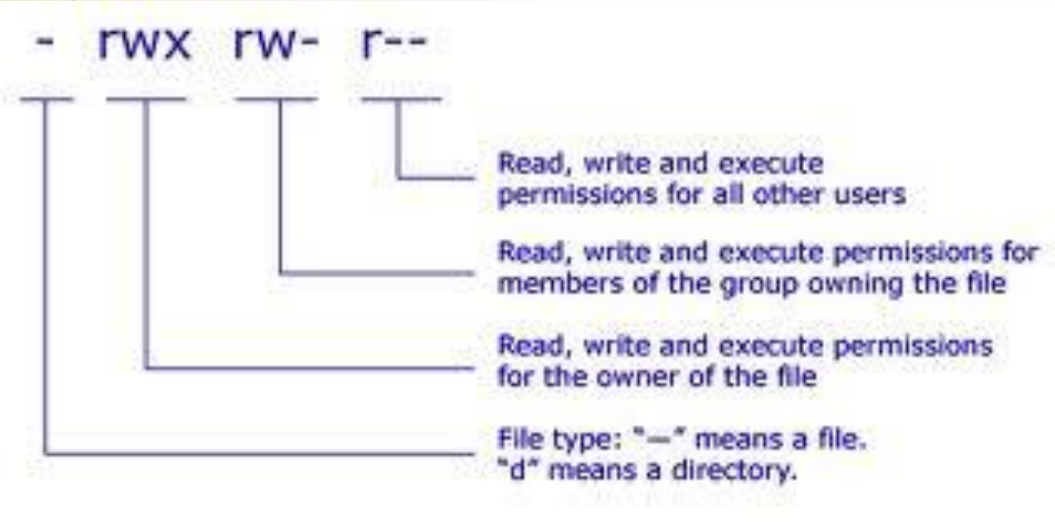


Rule Based Access Controls

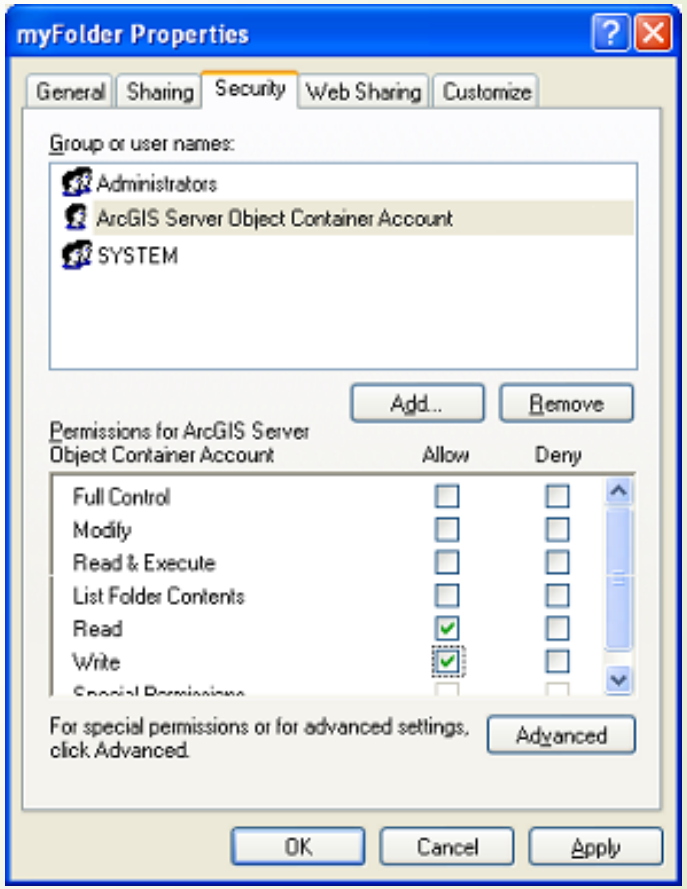
- Policy driven
- Used in routers and firewalls for network access
- Used in file systems “NTFS”
- Performs a “match” on the resource request based on a set of conditions
- Access Control Lists are the most common form of Rule Based Access Controls
- DAC system because the owner establishes the access controls
- Think Hardware

File Permissions

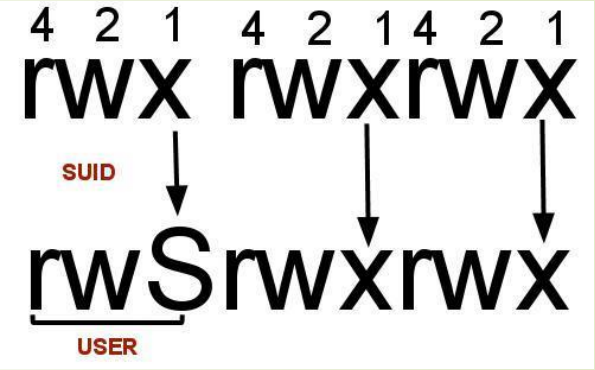
- **Unix/Linux**



- **Windows**



Privileged Programs



- UNIX/LINUX/MAC
  - SUID (set user ID)
    - Program preset to run with the authority of the program's owner
    - If the program is set to run as root, no matter who runs it, it runs as if root ran it.
  - SGID (set group ID)
    - Program preset to run with the authority of the program's group

Access Control Mechanisms

- Access Control Lists (ACLs)
- Capability Tables
- Constrained User Interfaces
- Temporal (Time Based) Isolation

Mary:
UserMaryDirectory – Full Control
UserBobDirectory – Write
Printer001 - Execute

SUBJECT	PROGRAM A	FILE 1	FILE 2
Joe	Execute	Read	Read/Write
Bob		Write	Read

Capability Table

Vulnerabilities of Security Architectures

- Most challenging threats:
  - Emanations
    - Control with TEMPEST and shielding (Faraday Cage)
  - State Attacks (i.e. Time of Check/Time of Use (TOC/TOU) attacks)
    - Identify possible covert channels
    - Analyze whether a channel actually exists
    - Verify if the channel creates security concerns
  - Covert channels
    - Avoid using filenames as input for system calls
    - Position files in their own folder where access is limited to the program that uses them

Mobile Device Key Security Areas

- Mobile devices need antimalware software
- Secure mobile communications
- Strong authentication
- Control 3rd party software
- Create separate, secured mobile gateways
- Require secure mobile devices
- Perform regular mobile security audits, penetration testing

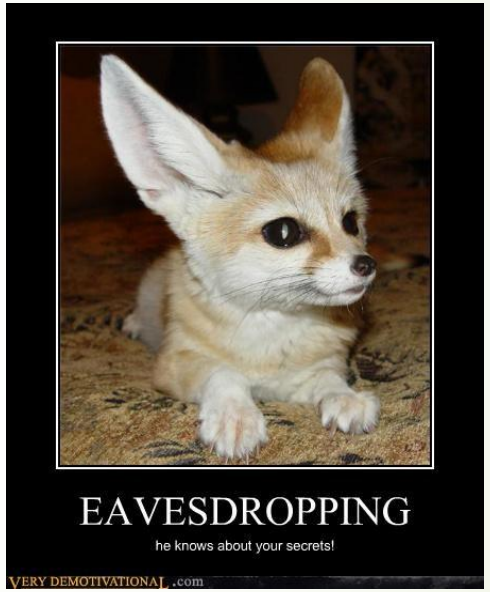
Personal Digital Assistants (PDA)s and Smartphones

- Personal Digital Assistants (PDA)
  - Being replaced by smartphones
  - Many are 802.11 and cellular capable
  - Easily stolen

- Smartphones
  - Convergence of cell phones and PDAs
  - Utilize remote wipe capability
  - Encrypt data
  - Easily stolen
  - Use secure wireless communications
  - Have auto discovery turned off

Cell Phone Abuse

- **Fraud**
- **Eavesdropping**



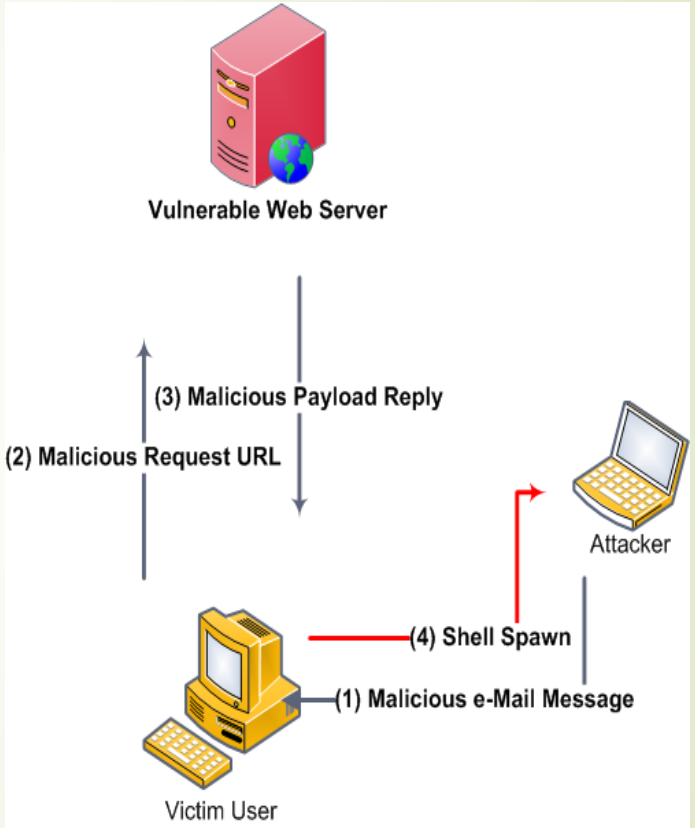
Single Point of Failure (SPOF)

- Security architects should conduct a single point of failure audit and the results should be compared to the outcomes of the Risk Analysis and Business Impact Analysis

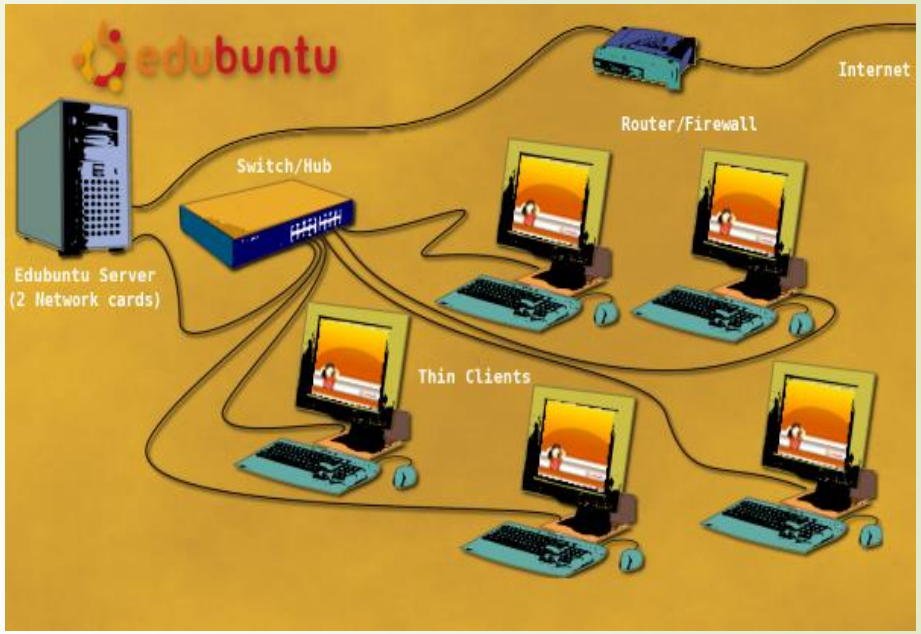
- SPOFs often occur in these areas:
  - Data connectivity
  - Network connectivity
  - Cluster communications (load balancing issues)
  - Application availability
  - OS availability (Virtualization)
  - Infrastructure

Client Based Vulnerabilities

- Client-Side Attacks
  - Caused by the user downloading malicious content
  - Reverse of server side attack
  - Attack initiates from victim



Design Principles



- Diskless workstations
- Thin clients/Thin processing/mainframes
- Thin storage
- Thick clients

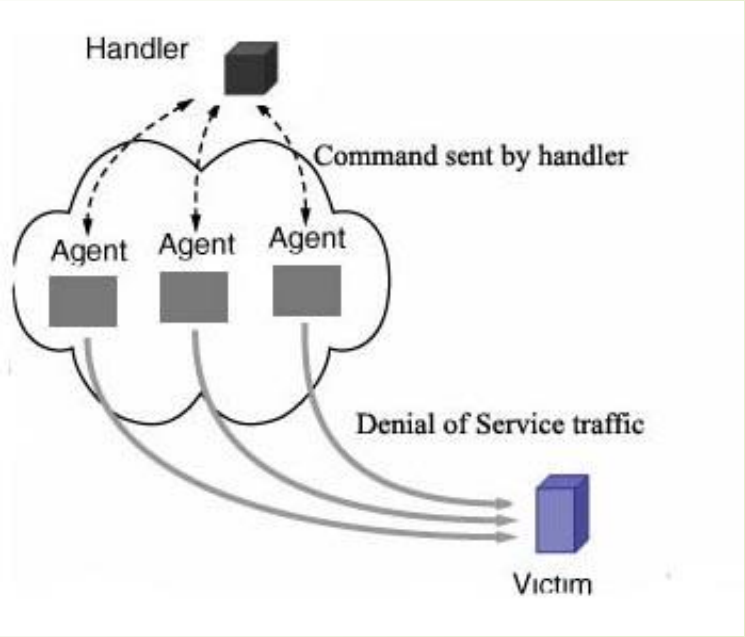
Bring Your Own Device (BYOD) and Mobile Device Management (MDM)

- Bring Your Own Device (BYOD)
  - Cultural shift towards using personnel electronics in the work place
  - Mobile devices not designed for enterprise security
  - Home and business network convergence

- Mobile Device Management (MDM)
  - Integrate remote disk wipe, account management, GPS/WIFI/Cellular location, updates, application management, device authentication and enrollment, archiving and integrity
  - Integrate secure web browser, VPN, whole disk encryption and key escrow, secure application store, and jailbreak detection

Server Based Vulnerabilities

- Server-Side Attacks (Client/server attacks)
  - A listening service is attacked directly by an attacker
  - Defense:
    - Firewalls
    - Patching
    - System hardening
    - Defense in depth



Data Warehousing and Data Mining

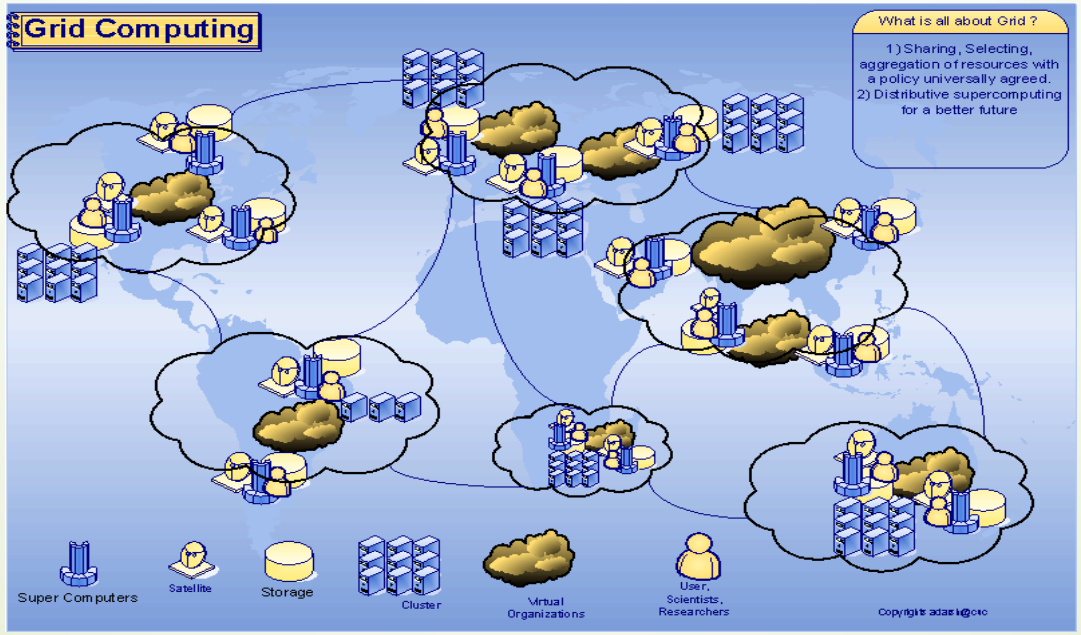
- Data Warehousing
  - Combines data from multiple databases
  - Data is extracted and transferred to central store
  - Online Analytical Processing (OLAP)
- Inference
- Aggregation
- Data Mining
  - Massaging/Analyzing data
  - Metadata (data about data)
  - Can produce previous unseen relationships

Distributed Systems

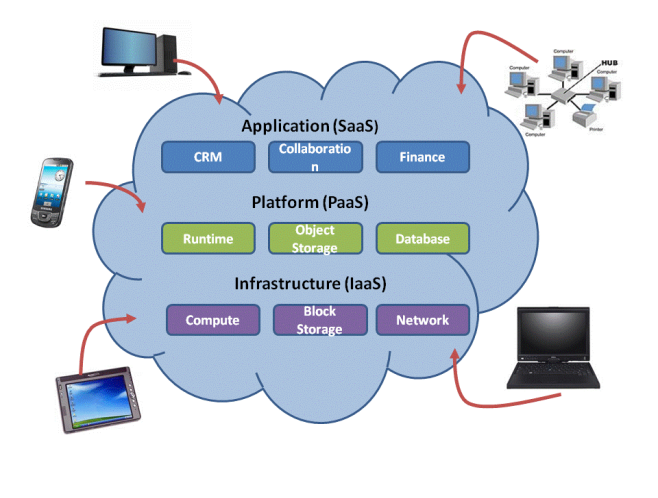
- Opposite of centralized systems (i.e. mainframes and thin clients)
- Client/Server Architecture
- Peer-to-Peer Systems
- Challenges:
  - Coordinating resources
  - Lacks a central authority
  - Authorization
  - Difficult to control security vulnerabilities

Grid Computing

- Harness the power of computer cycles not being utilized
- Load balance processing among multiple computers



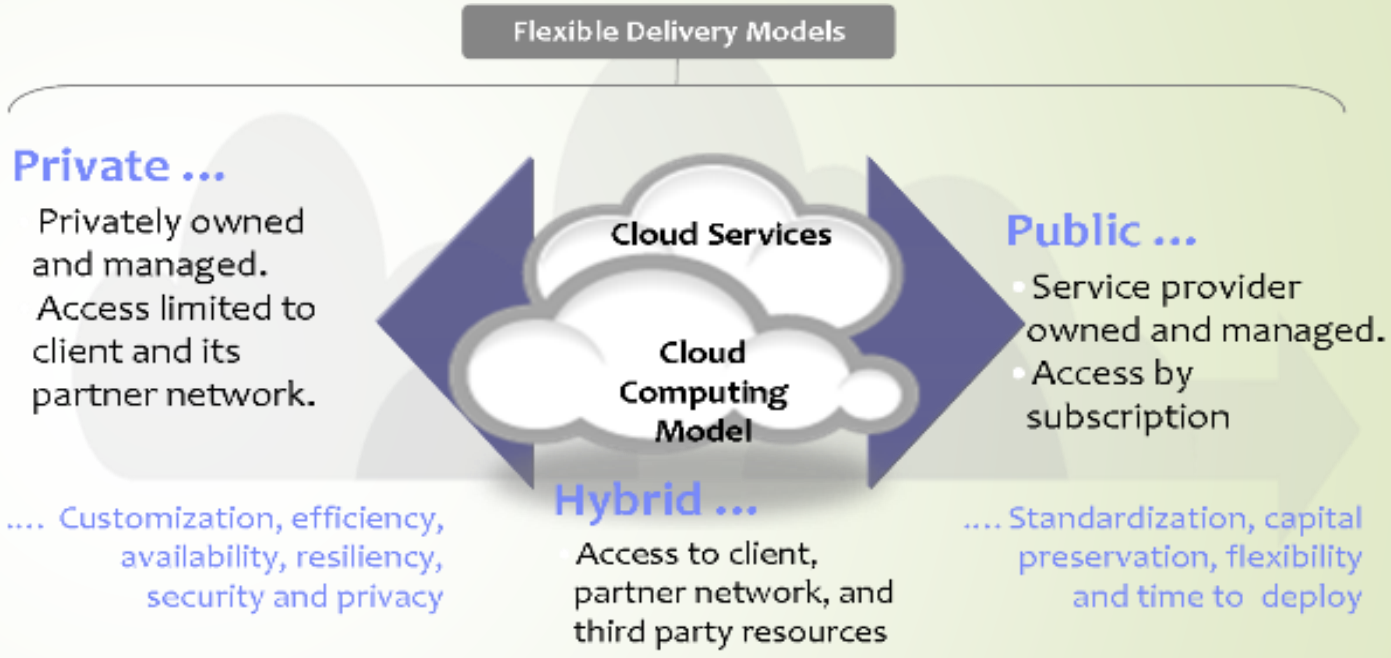
Cloud Computing



- Cloud Computing is "in the cloud" (internet)
  - SW, data access, and storage services that do not require user knowledge of the location and configuration of the system delivering services
  - Three layers
    - Software as a Service (SaaS) – application
    - Platform as a Service (PaaS) – platform
    - Infrastructure as a Service (IaaS) - infrastructure
  - Example: web based e-mail like Yahoo or Hotmail, ISP's

Cloud Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud



Cloud Computing Vulnerabilities

- All Yours Eggs in One Basket (DoS)
- Weak Authentication Methods (authentication attacks)
- Encrypting Data in the Cloud
- Chain of custody is difficult to maintain
- Data Extraction
- Man in the Middle attacks

Cloud Security Guidelines

- Carefully plan the security and privacy aspects of cloud computing solutions before implementing them.
- Understand the public cloud computing environment offered by the cloud provider.
- Ensure that a cloud computing solution—both cloud resources and cloud-based applications—satisfy organizational security and privacy requirements.
- Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.

Key Encryption Concepts and Definitions

- Cryptography
- Cryptanalysis
- Cryptology
- Algorithm
- Plaintext/Cleartext
- Ciphertext/Cryptogram
- Encipher/encode
- Decipher/decode
- Avalanche Effect
- S-Box
- Key (cryptovariable)
- Key Zeroization

Key Encryption Concepts and Definitions

- Work Factor
- Initialization Vector/Salt
- Confusion
- Diffusion
- Zero Knowledge Proof
- Frequency Analysis
- Steganography
- Rounds
- Monoalphabetic
- Polyalphabetic
- SP-Network

Encryption Systems

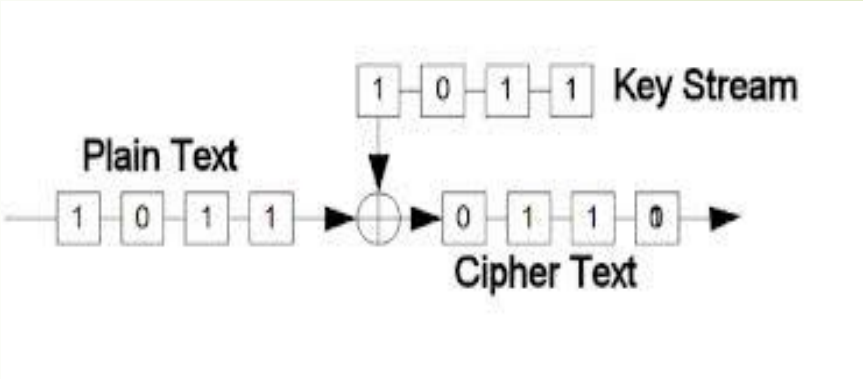
- Substitution Cipher (confusion)
- Transposition Cipher (diffusion)
- Null Cipher
- Playfair Cipher
- Rail Fence Cipher
- Vigenere Cipher
- Modular Mathematics
- A book cipher
- A running key cipher
- One-Time Pad

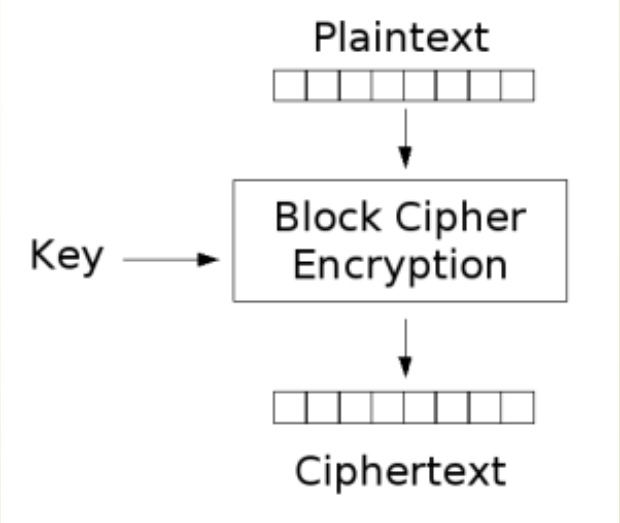
Symmetric Cryptography

- Both parties share the same key (kept secret)
- Before communications begin, both parties must exchange the shared secret key
- Faster than asymmetric cryptography
- Best suited for bulk encryption
- N(N-1)/2 = number of keys needed
- a.k.a. Secret, Single, Conventional, Session, Shared, Private, File Encryption Key (FEK)

Symmetric Algorithms

- Two types of symmetric algorithms:
  - Stream Cipher / Stream Algorithm
    - Works on one bit (or byte) at a time
  - Block Cipher / Block Algorithm
    - Works on blocks of bits



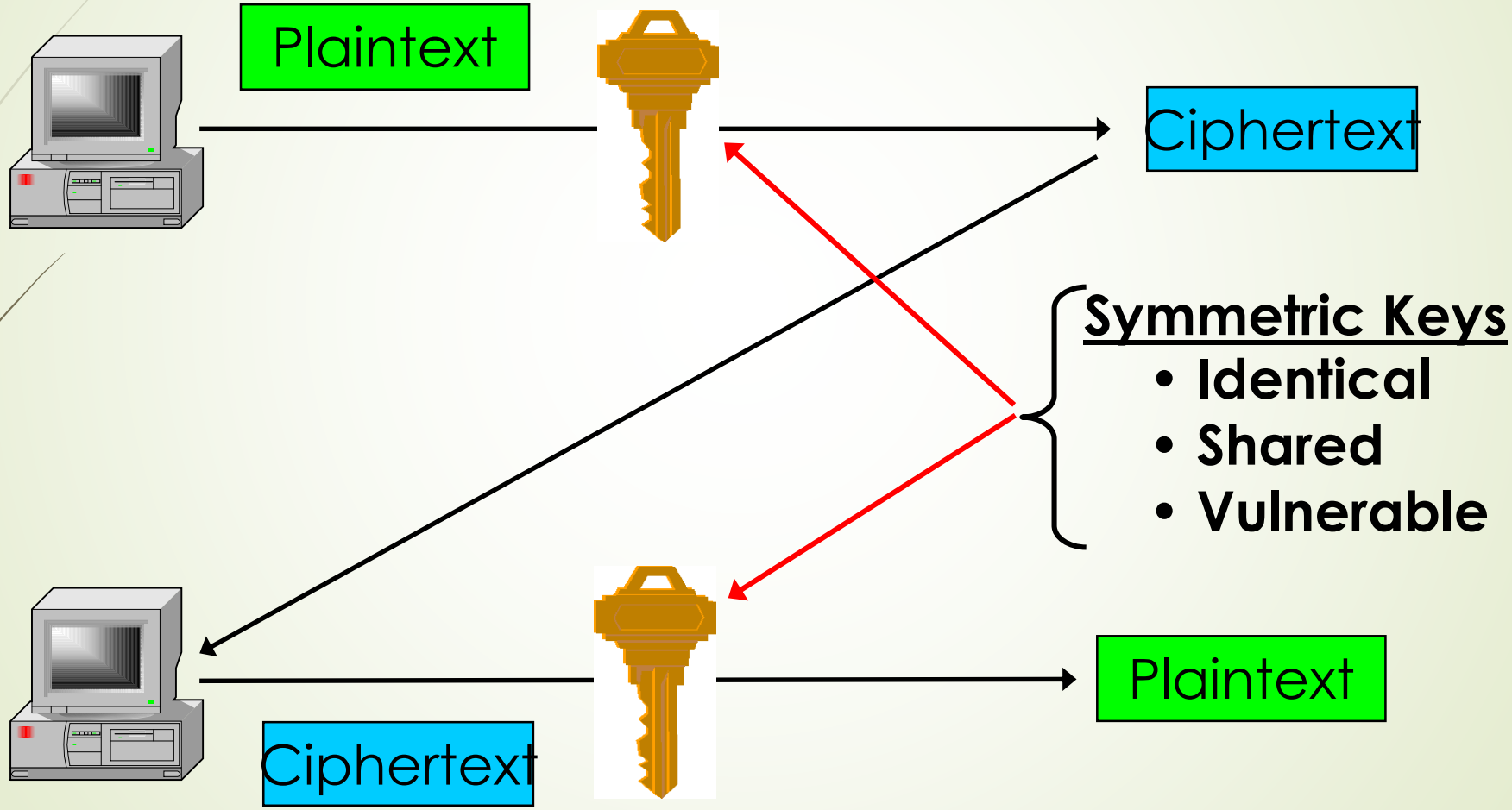


Stream Cipher XOR Operation

- **Treats message as a stream of bits**
- **Performs mathematical XOR function on each individual bit**
- **Uses keystream generators, producing a stream of bits that is XORed with plaintext bits to generate ciphertext**

Converted Plaintext	0101 0001
Keystream	0111 0011
Output of XOR	0010 0010

Symmetric Key Encryption



Symmetric Algorithms Memory Tool

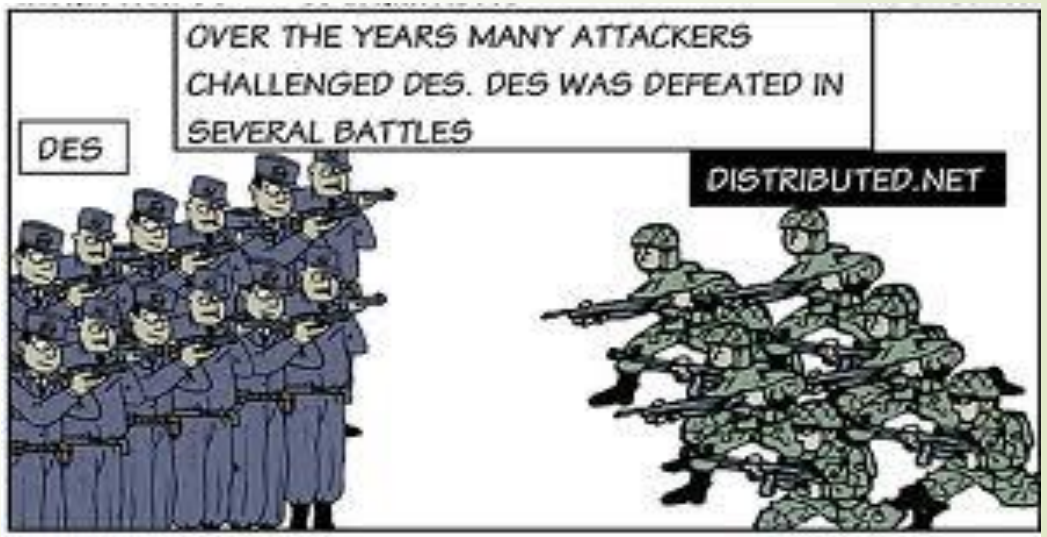
- **C ast 128 / 256 (64 bit/128 bit)**
- **3 DES 2-112 bit / 3-168 bit (48 Rds)**
- **2 fish 128 bit**
- **B lowfish 64 bit**
- **R C 4 (Stream and WEP) 5,6 (Block)**
- **A ES 128 bit Block (128/10)(192/12)(256/14)**
- **I DEA 64 bit Block / 128 key**
- **D ES 64 bit Block / 56 bit key (8 bit parity)**
- **Safer+, Safer++**

Lucifer

- Developed by IBM to protect non-classified information
- First ever block cipher
- Uses a 128-bit key on 16 rounds of encryption
- Suffers from weak key generation
- NSA modified algorithm to use a key size of 64 bits (8 parity; 56 length)
  - Called this modified algorithm DEA (Data Encryption Algorithm)

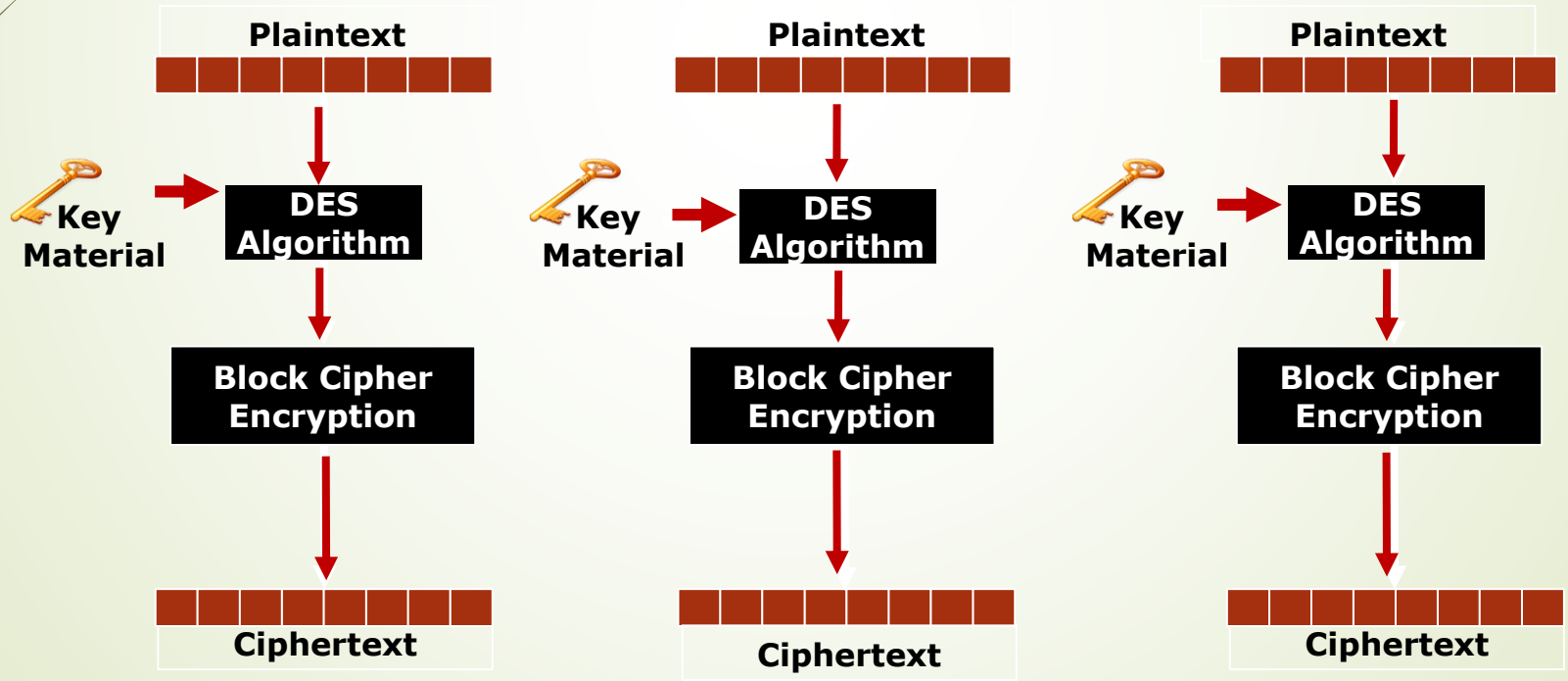
Data Encryption Standard (DES)

- DEA is the algorithm for DES
- Uses a 56 bit key with 8 bits of parity (total 64 bits)
- Encrypts 64 bit blocks of text
- Most widely used block cipher
- 5 Block Models



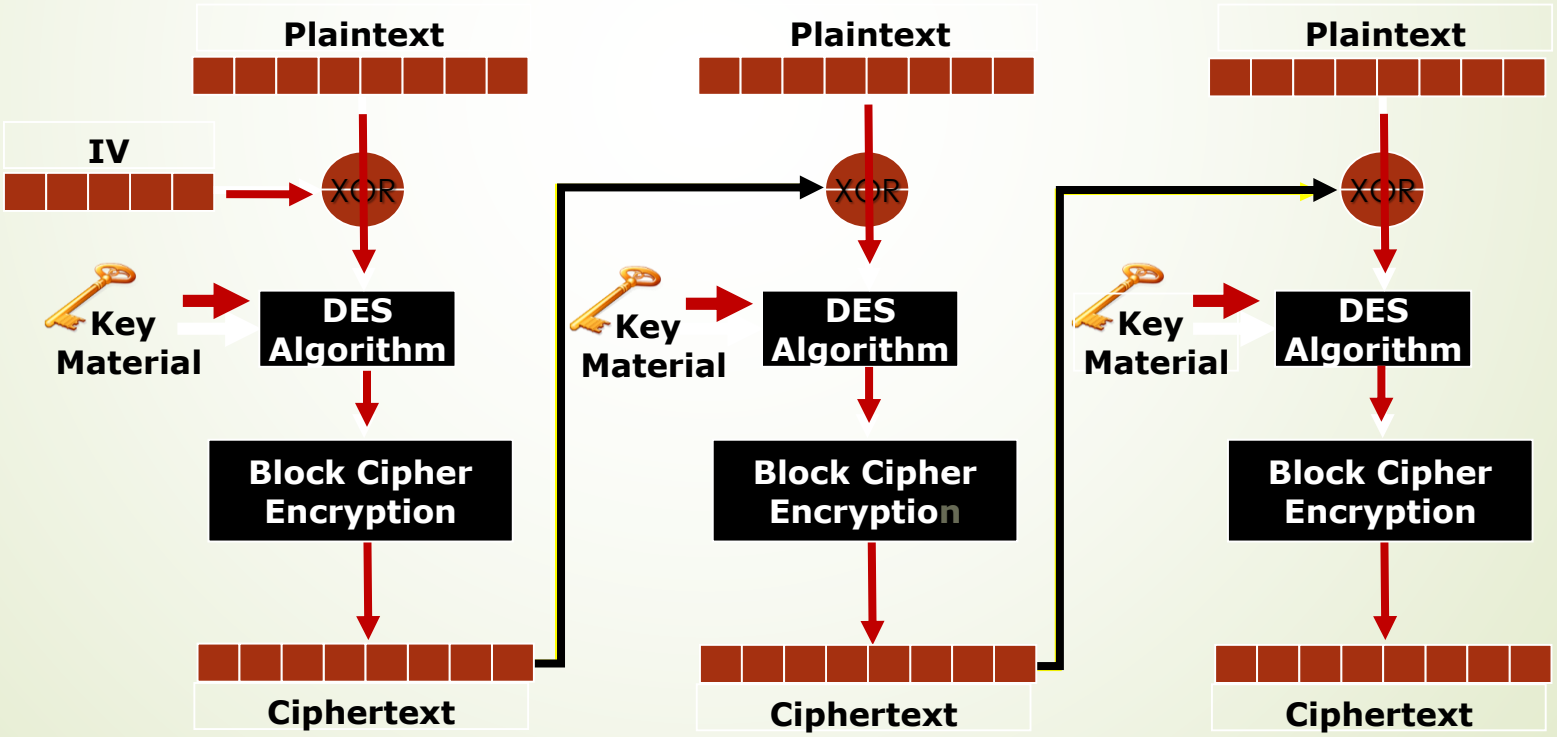
Electronic Code Book (ECB)

- Each block encrypted independently (parallelization)
  - Processes 64-bits at a time using the same key
  - Decrypting starts at beginning of ciphertext (reverses the encryption process)



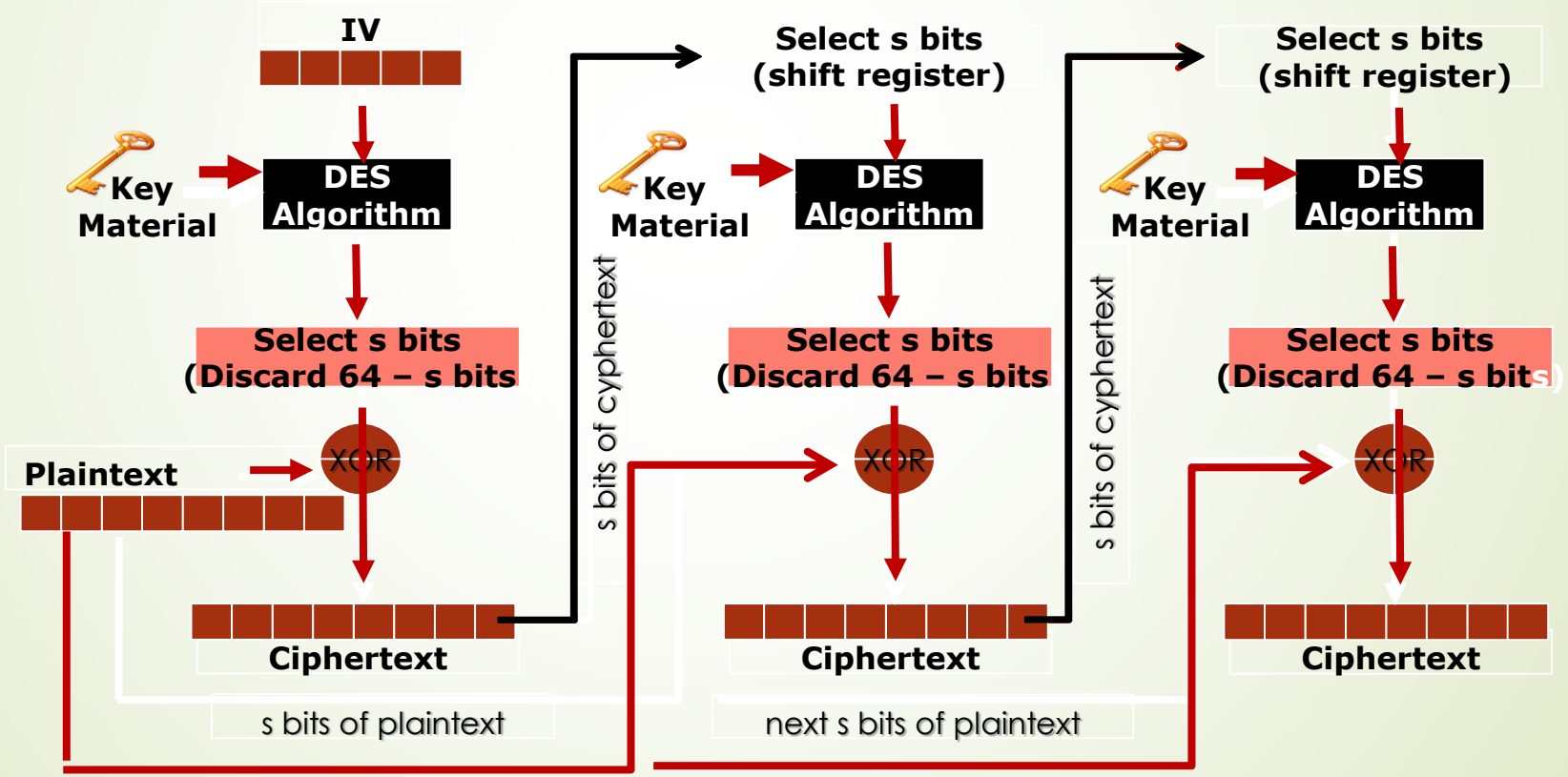
Cipher Block Chaining (CBC)

- Most common mode
- Loaded sequentially and XORed using 64-bit IV (blocks)



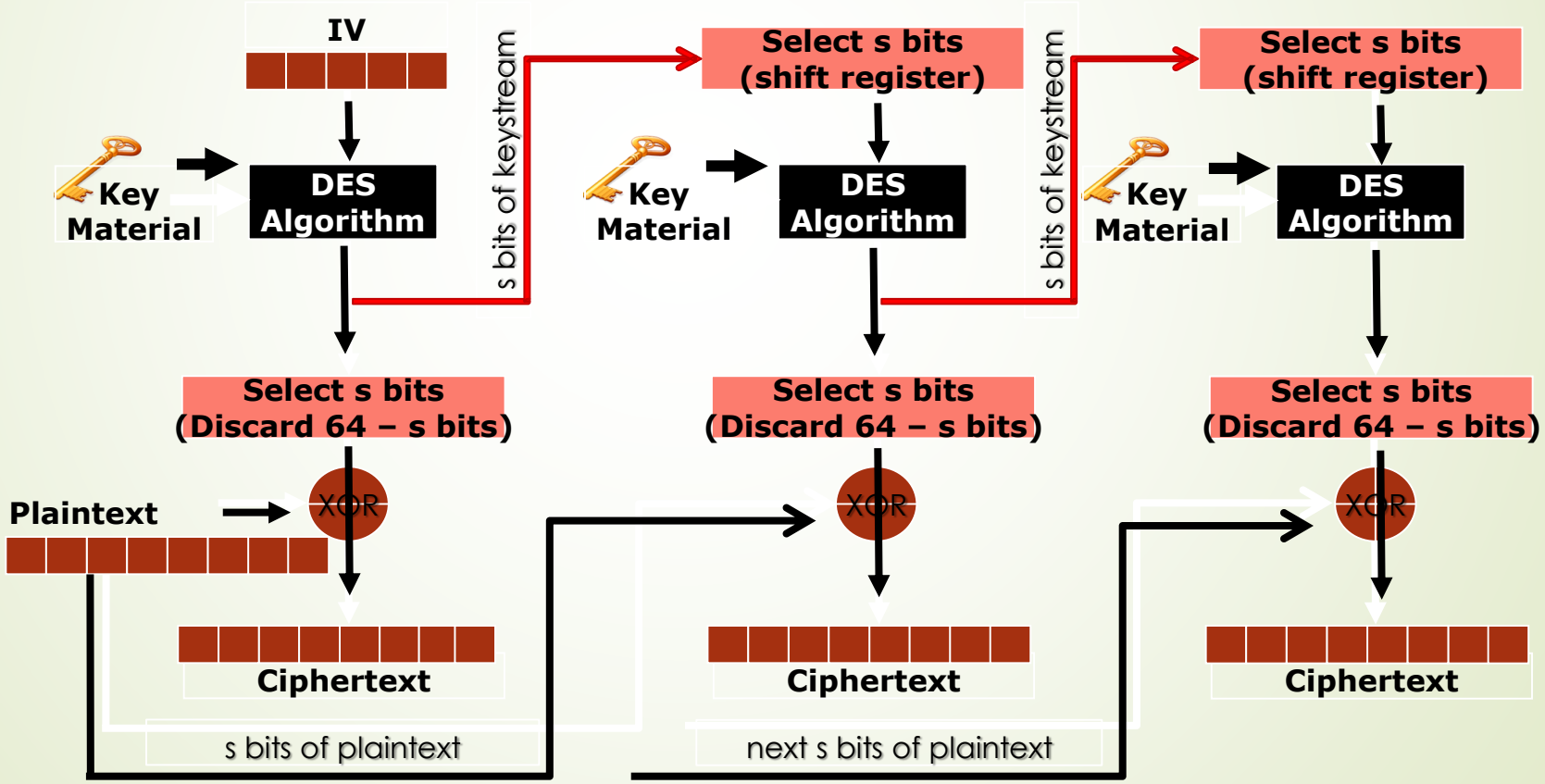
Cipher Feedback (CFB)

- Emulates a Stream Cipher: Data is encrypted in units smaller than the block size (bits or bytes)



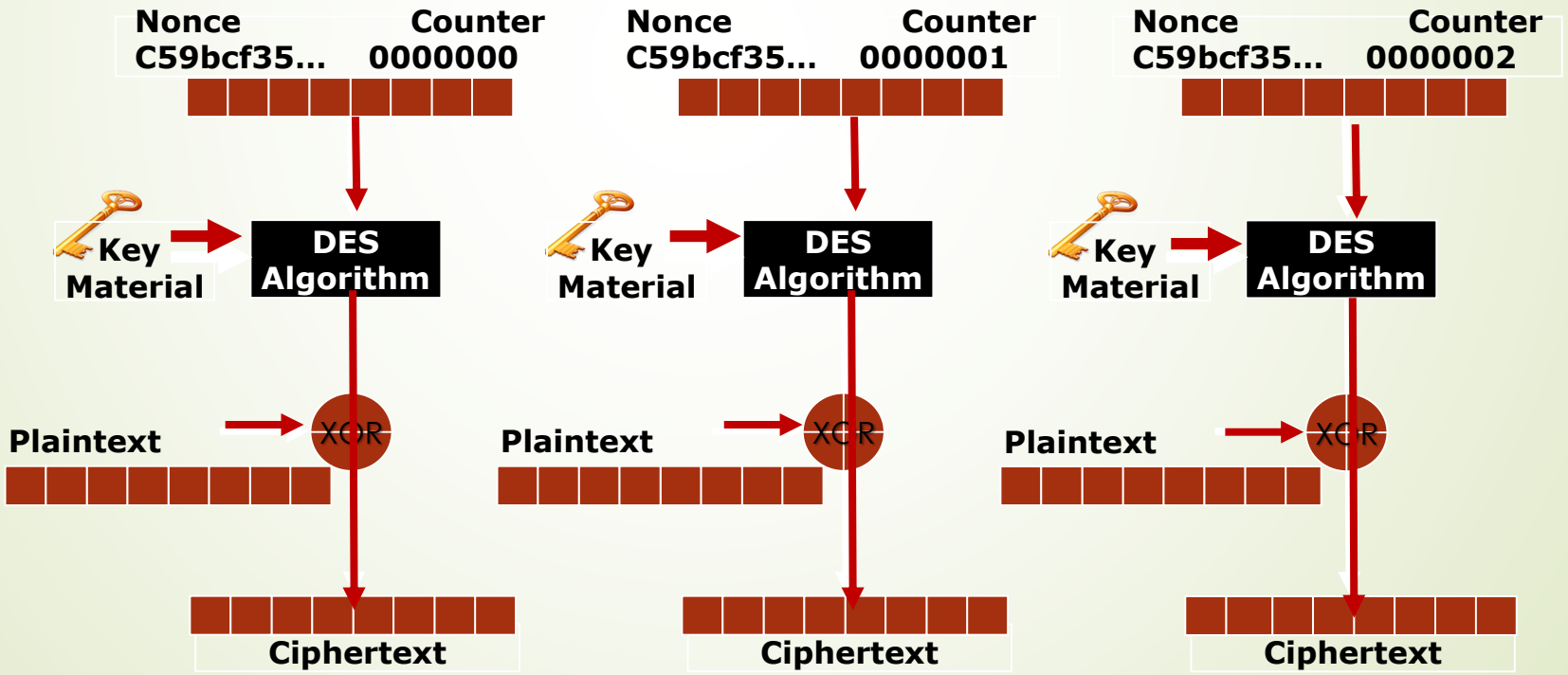
Output Feedback (OFB)

- Similar to CFB, except quantity XORed with each plaintext block is generated independently of plaintext and ciphertext



Counter Mode (CTR)

- Similar to OFB mode: Instead of a static IV, a counter is incremented with each data block
- Each block XORed with a unique keystream value

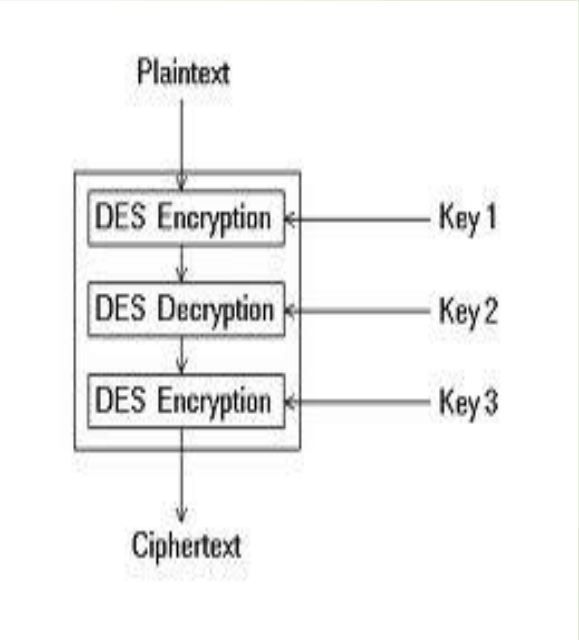


Mode Comparison

Mode	Type	IV	Error Propagation
ECB	Block	N	N
CBC	Block	Y	Y
CFB	Stream	Y	Y
OFB	Stream	Y	N
CTR	Stream	Y	N

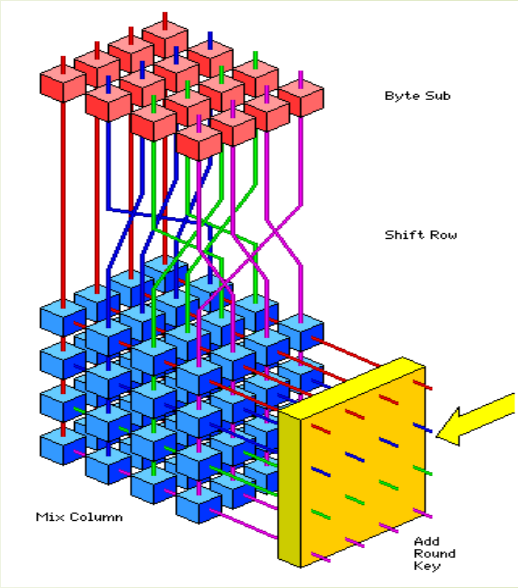
Triple-Data Encryption Standard (3DES)

- Developed as a quick fix for DES weaknesses
- 3DES uses 48 rounds in its computations
- Takes up to 3 times longer to encrypt / decrypt
- May use two or three keys:
  - EEE2 ~ Two Key
  - EDE2 ~ Two Key
  - EEE3 ~ Three Key
  - EDE3 ~ Three Key
- Effective Strength = 112 (2) / 168 (3)



Advanced Encryption Standard (AES)

- Replacement for DES/3DES
- Uses the Rijndael algorithm (beat out: RC6, serpent, mars, twofish)
- Only Block size: 128 (not 192 and 256) per FIPS 197
- Variable Key sizes: 128, 192, and 256
- Uses a variable number of rounds (10, 12, 14)
- 4 major operations that provide confusion, diffusion, and XOR
  - Subbytes
  - Shift Row
  - Mix Columns
  - Add Round Key



Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

- **AES CCMP requires 128 bit key and 128 bit block size**
- **48 bit IV to minimize replay attacks**
- **CBCMAC used to produce Message Integrity Code (MIC)**
- **Included in 802.11i standard**
- **AES-CCMP produces a higher level of security over past protocols**

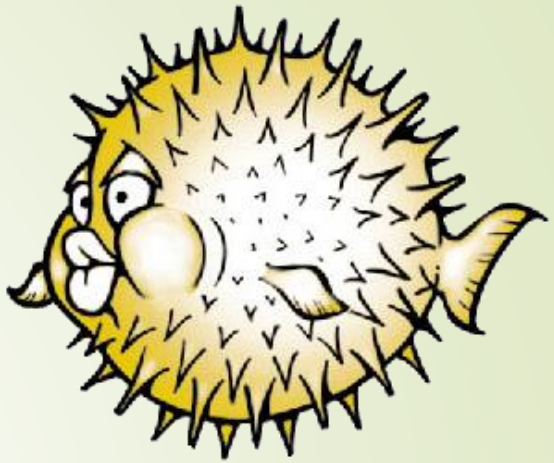
International Data Encryption Algorithm (IDEA)

- Uses a block cipher and operates on 64-bit blocks of data
- Uses 128 bit key and is faster than DES
- 8 rounds
- Used in PGP and other encryption software
- Patented (ends 2010) and licensing fees stopped it from replacing DES
- Currently; no successful practical attacks

Carlisle Adams and Stafford Tavares (CAST)

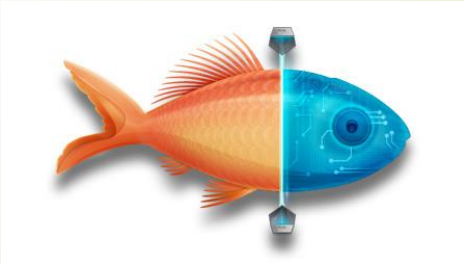
- Developed by Carlisle Adams and Stafford Tavares
- Cast-128
  - 64-bit block cipher
  - Uses keys between 40 and 128-bit lengths
  - Performs 12 to 16 rounds of operations
- Cast-256
  - 128-bit block cipher
  - Uses keys of 128,192,160, 224, and 256-bit lengths
  - Performs 48 rounds of operations

Other Symmetric Standards



- **Blowfish**
  - **Block cipher: 64-bit blocks of data**
  - **Variable key length from 32 bits up to 448 bits (128 bit is default)**
  - **Performs 16 rounds of operations**

- **Twofish**
  - **Block cipher: 128-bit blocks of data**
  - **Variable key length from 128, 192, to 256 bits**
  - **Performs 16 rounds of operations**



Other Symmetric Standards

- SAFER (secure and fast encryption routine)
  - 64 bit input block (Safer-SK64) or 128 bit input block (Safer-SK128)
  - Used in Bluetooth for key derivation (block cipher)

- RC4, 5, 6
  - Developed by Ron Rivest
  - Supports SSL and WEP protocol standards
  - RC4 most widely used software stream cipher
  - RC5 and RC6 are block ciphers
  - RC6 lost out as replacement for DES

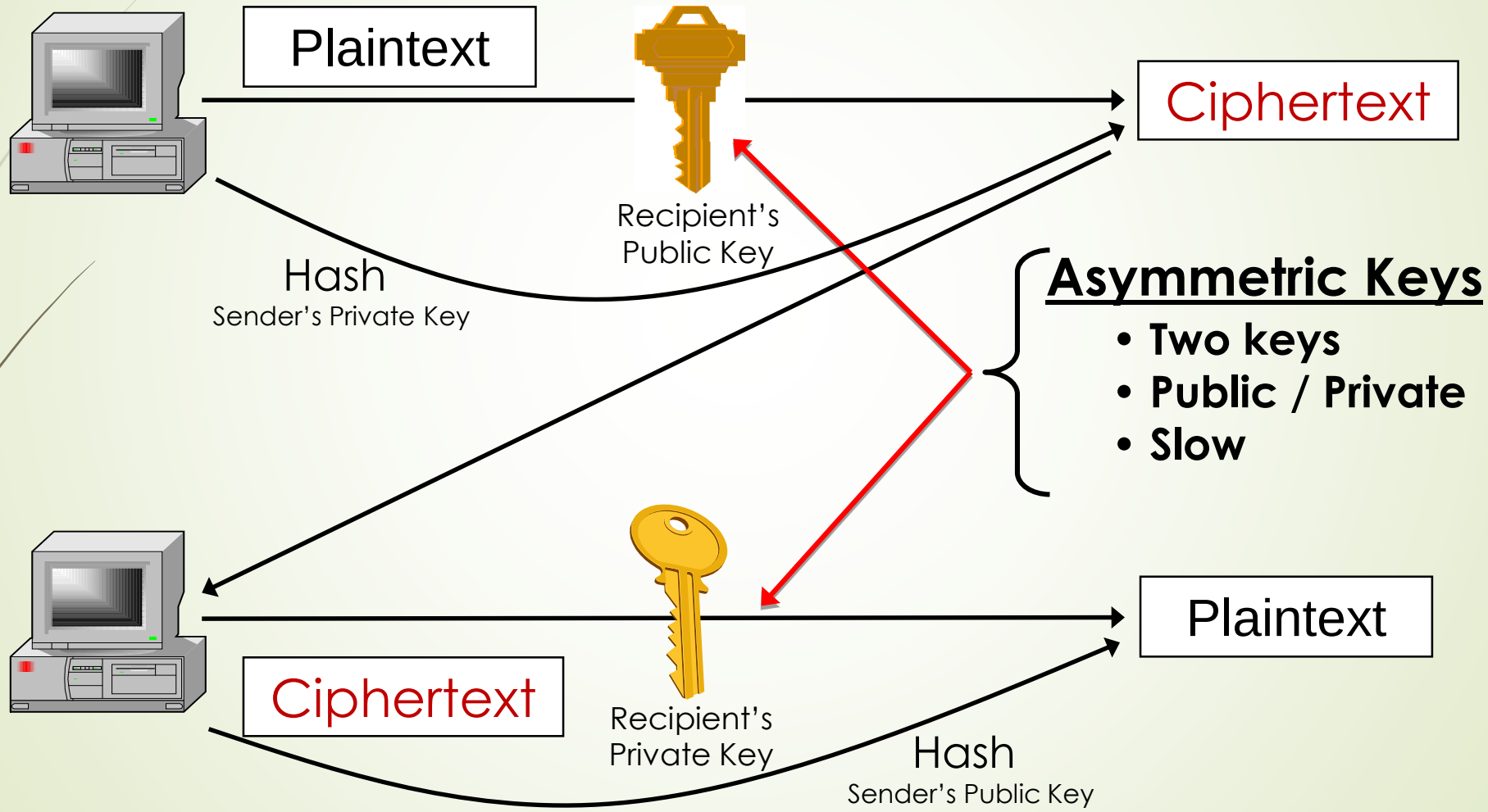
Symmetric Algorithms

- Advantages
  - Very fast and secure
  - Many algorithms can be implemented in either hardware or software and are available at no cost to the user
- Disadvantages
  - Key management
  - The number of keys needed can be very large
  - n(n-1)/2 where n = number of users or nodes

Escrowed Encryption & the Clipper Chip

- Escrowed Encryption
  - Trusted 3rd party keeps copy of private key pair
  - Provide a balance between privacy and the needs of law enforcement
- Clipper Chip
  - Used 80 bit symmetric encryption with the Skipjack algorithm (classified up to 1998)
  - Was the Escrowed Encryption Standard (EES) in 1993 but abandoned in 1996
  - Project is now abandoned

Asymmetric Key Encryption



Asymmetric Keys

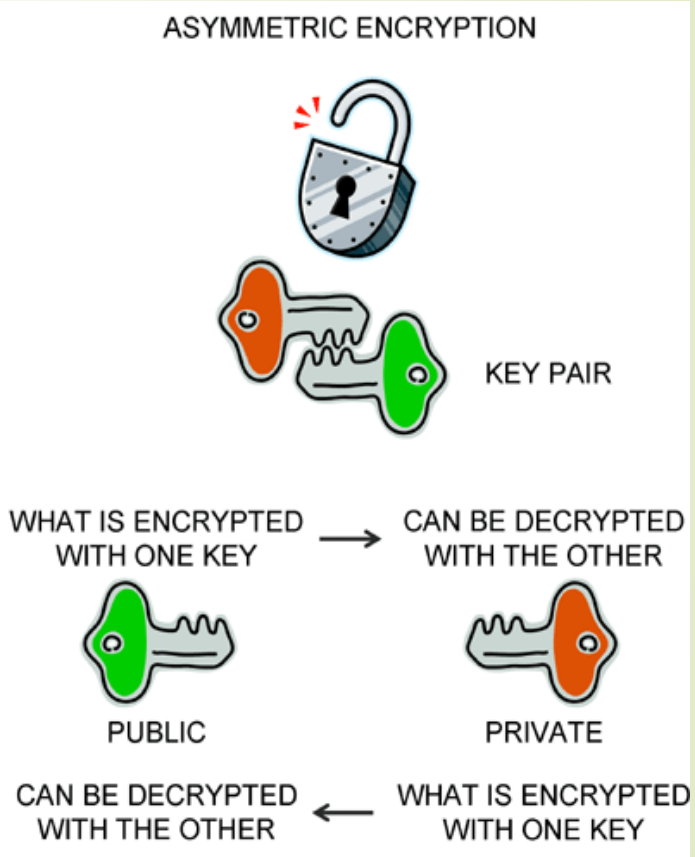
- **Two keys**
- **Public / Private**
- **Slow**

Asymmetric Algorithms

	Encr	DSig	KEx
D iffie-Hellman			X
E CC	X	X	X
E lGamal	X	X	X
R SA	X	X	X
DSA/DSS		X	

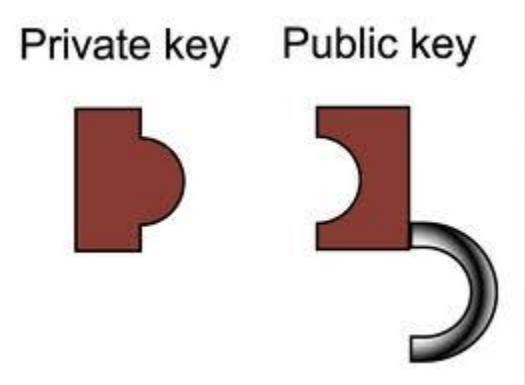
Asymmetric Algorithms

- Uses different keys for encryption and decryption
- Each user has two keys: public & private key
  - Both keys together are called the key pair
  - Keys are mathematically related
  - Public key is derived from private key
- Public key made available to anyone
- Private key kept secret
- Also known as public key algorithms



Asymmetric Algorithms

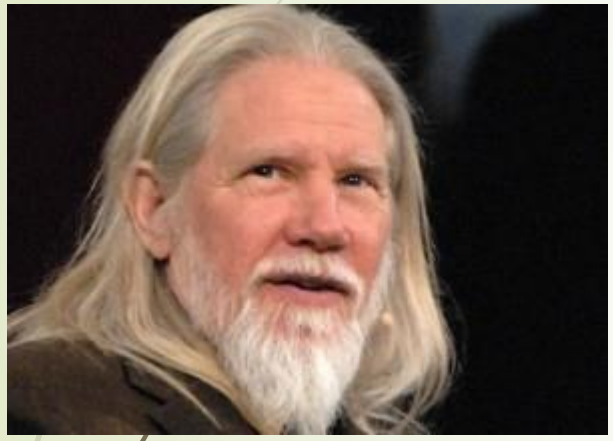
- Encrypting data with the sender's private key provides proof of origin, without confidentiality
  - Ensures the message has come from the stated sender
  - Open message format
- Signing a message with the sender's private key creates a digital signature
  - Provides nonrepudiation



Rivest, Shamir, Adleman (RSA)

- Based on factoring of large prime numbers (integer factorization)
  - Which **Prime Number Times Which Prime Number Equals 49,418,527**
    - Example: **6269 x 7883 = 49,418,527**
- Provides Encryption, Digital Signatures, and Key Exchange
- Variable key length and block size 512 to 4096
- Strong, but very slow in speed
  - 100 times slower than conventional encryption in software
  - 1,000 – 10,000 times slower that conventional encryption in hardware

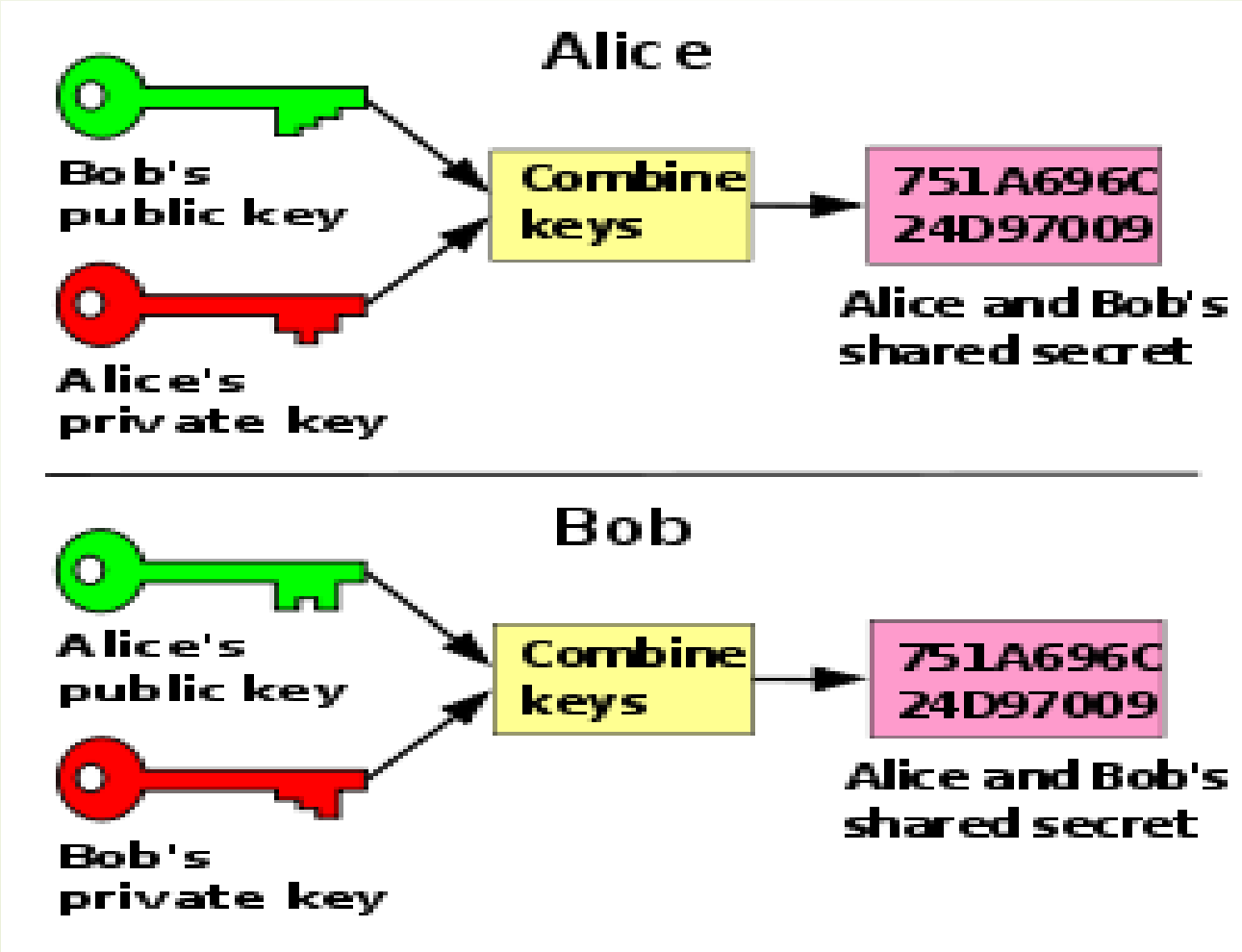
Diffie-Hellman Algorithm



Whitfield Diffie

- First public-key agreement algorithm
- Not used for message encryption or digital signatures (only used for key exchange)
- Uses discrete logarithms containing large prime numbers
  - A logarithm is the opposite of exponentiation (7 to the 13th power)
    - Example: 96, 889,010,407 is 7 to what power? Find the logarithm (more difficult)
- Requires both the sender and receiver of a message to have key pairs

Diffie-Hellman Key Agreement Protocol

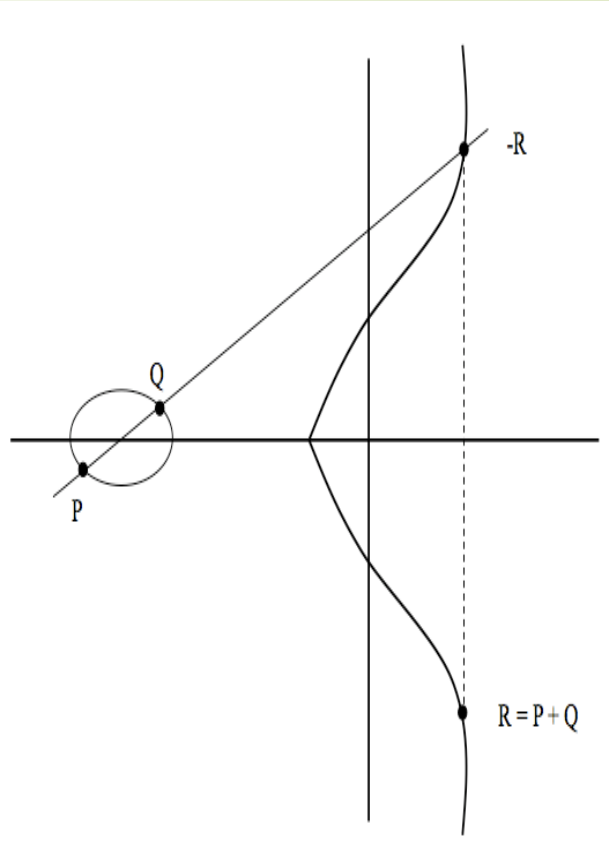


ElGamal

- Based upon the Diffie-Hellman
- Provides Encryption, Digital Signatures, and Key Exchange
- Discrete logarithms (easy to reverse re-engineer)
- Main drawback is performance (slower than other comparable algorithms)

Elliptical Curve Cryptography

- Provides Encryption, Digital Signatures, and Key Exchange
- Highest strength per bit of key length
- Uses shorter keys, most efficient asymmetric algorithm
- An ECC key of 160 bits is equivalent to a 1024-bit RSA key
- Used in Wireless Devices
- Suitable for hardware applications



Asymmetric Key Encryption

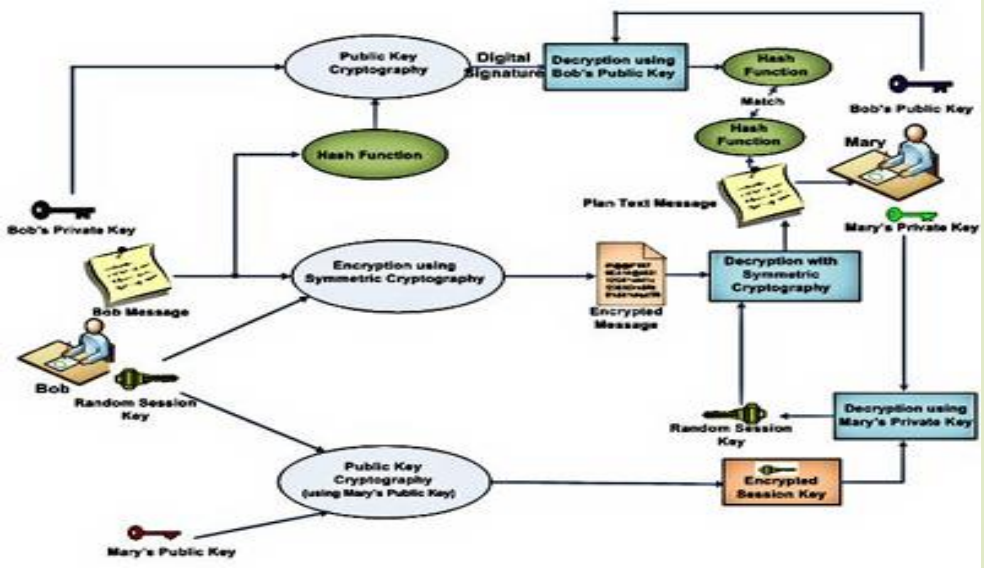
- Pros: Key Management
  - Two keys (public and private): N*2
  - Private key cannot be derived from the public
  - Offers Non-repudiation, Confidentiality, Integrity
- Cons: Speed/File size
  - Computationally intensive
  - Hundreds to thousands times slower than symmetric key algorithms

Symmetric Key Lengths vs. Asymmetric Key Lengths

Symmetric Key Length	Symmetric Algorithm	Discrete Logarithm Equivalent Key Length	Factoring Prime Number Equivalent Key Length	ECC Equivalent Key Length
112	3DES	2048	2048	224-255
128	AES	3072	3072	256-283
192	AES	7860	7860	384-511
256	AES	15,360	15,360	Above 512

Hybrid Encryption Methods

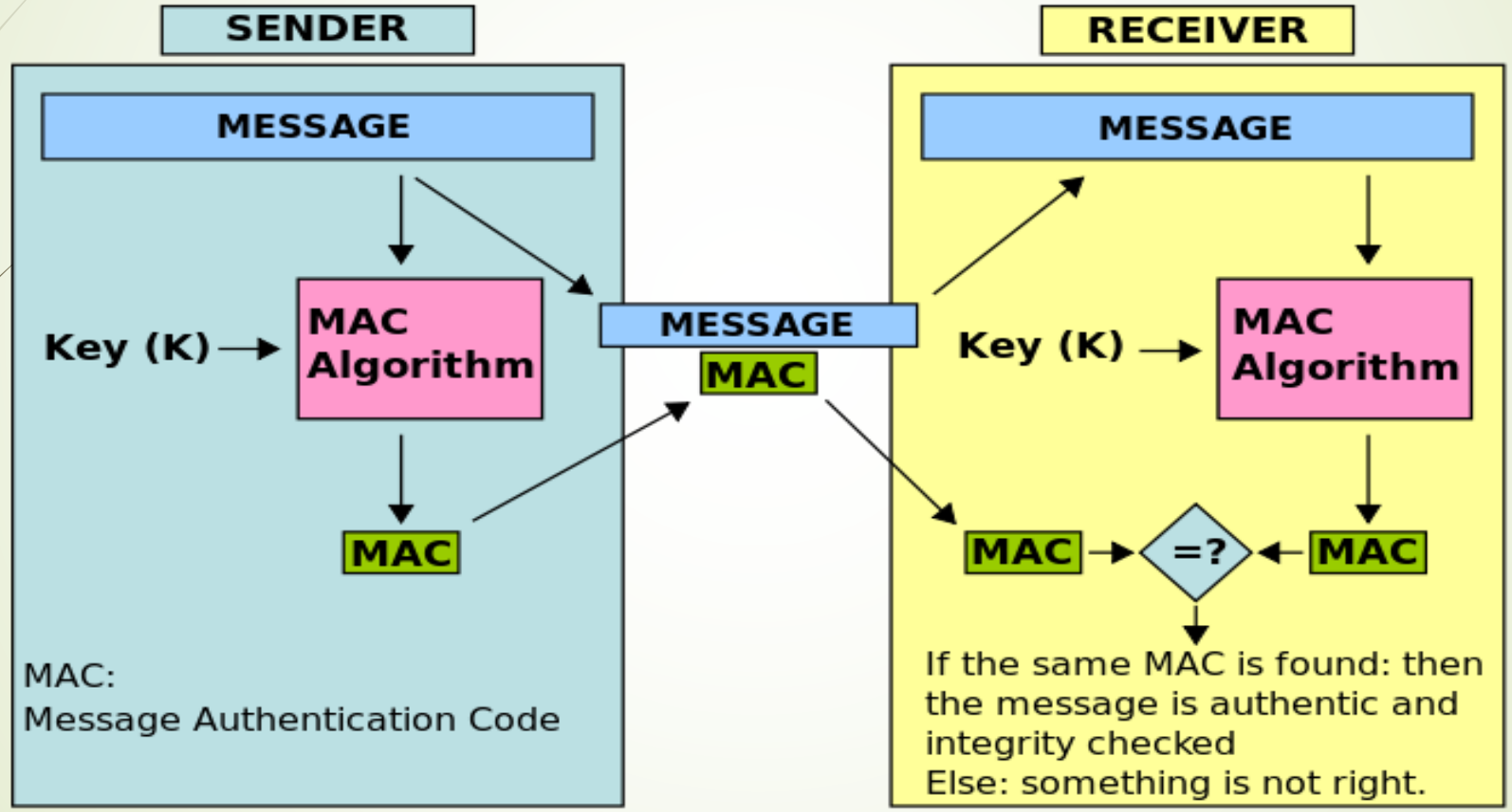
- Method for maintaining integrity, confidentiality, and authentication
- Constructed using two or more cryptosystems:
  - Hashing for Integrity
  - Symmetric for Bulk Encryption
  - Asymmetric for Key Encapsulation
- Used in:
  - SSL
  - Email
  - Key Exchange



Message Authentication Codes

- aka: Message Integrity Code; Modification Detection Code; Cryptographic Checksum
- Used to verify integrity and data origin (two ways):
  - Value generated by running a message through a block cipher (CBC) or a hash function
- Recipient creates a MAC using the same secret key and compares it to the MAC received
- Requires the sender and the receiver to share a secret key

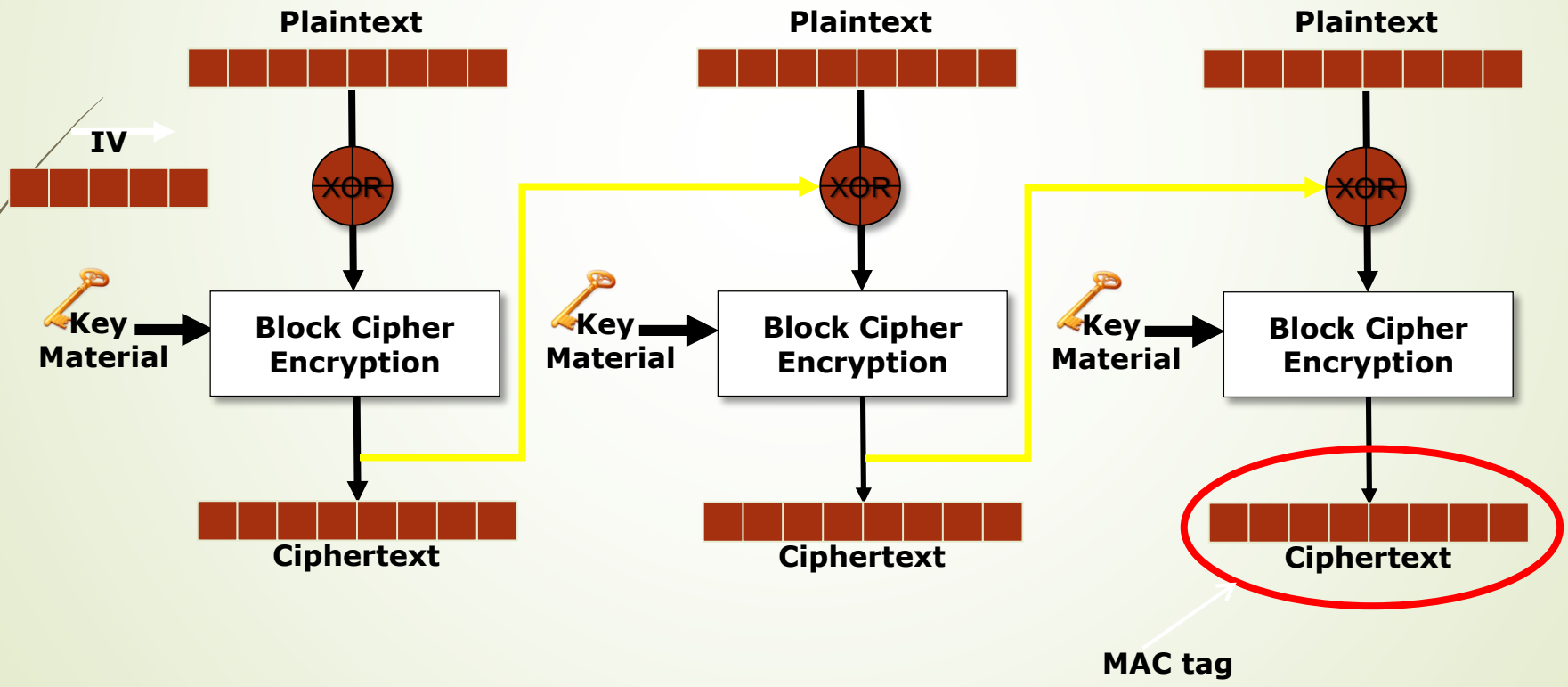
Message Authentication Codes



Message Authentication Codes (CBC-MAC and CMAC)

- Constructed using any block cipher
  - AES or DES commonly used
- Message encrypted in CBC mode
- MAC tag is the last block of cipher text generated by the algorithm (16 - 64bits)
- Size of the MAC is limited to the size of the last block
- CMAC is stronger than CBC-MAC
  - Pads the last block and uses 2 keys
- Slower than HMAC

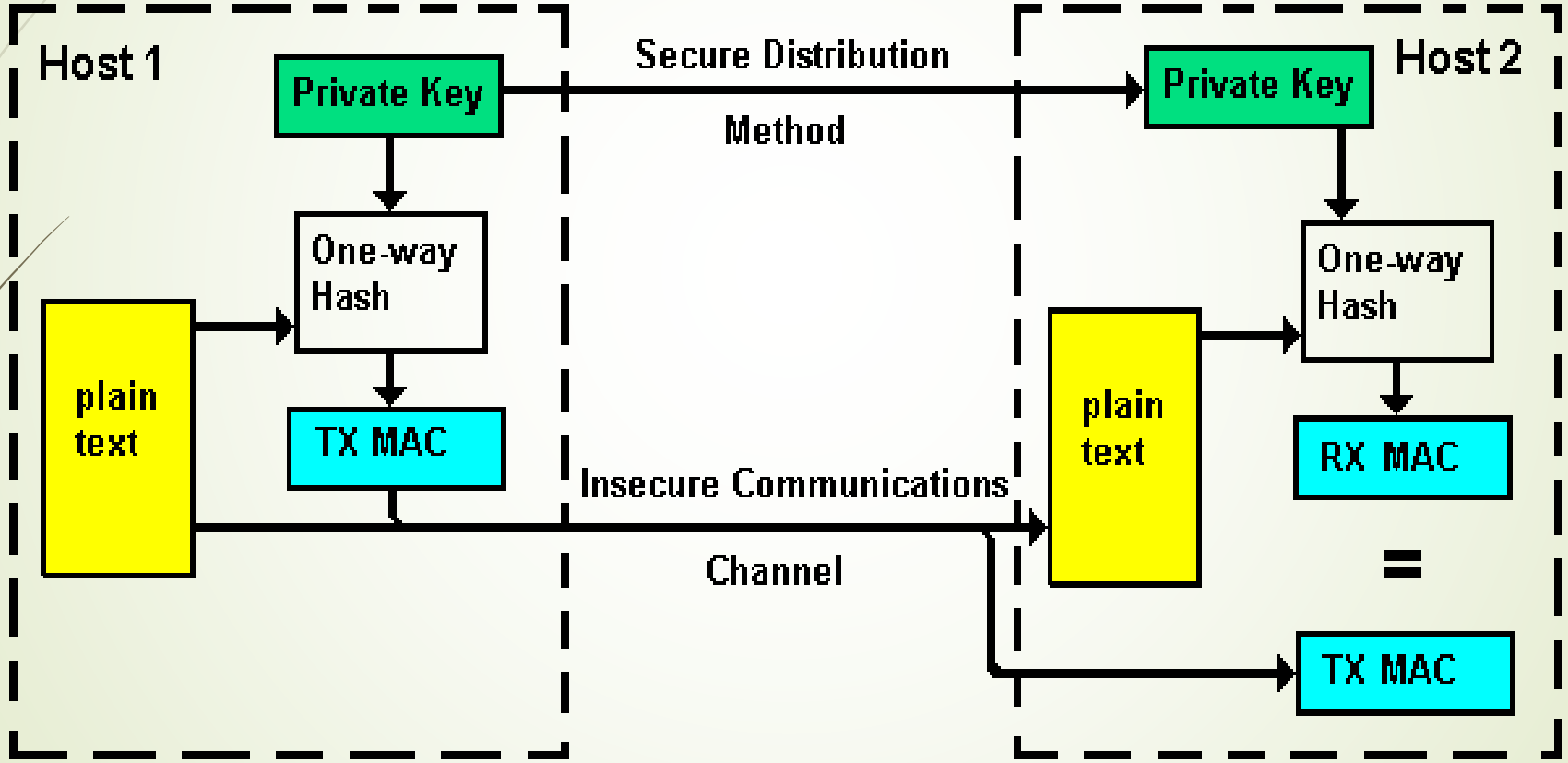
Message Authentication Codes (CBC-MAC and CMAC)



Hashed Message Authentication Codes (HMAC)

- Type of MAC calculated using a hash function in combination with a secret key
- The shared secret key is appended to the data to be hashed
- Uses MD5 or SHA-1
- Used in Internet Protocols such as IPSec, SSL/TLS, and SSH
- Creates a more rapid message digest (CBC-MAC and CMAC uses block chaining, which is slow)

Hashed MACing (HMAC)



Software and System Vulnerabilities & Threats

- **Web-Based Applications**
- **Extensible Markup Language (XML)**
- **Security Assertion Markup Language (SAML)**
- **Open Web Application Security Project (OWASP)**
  - **Provides a framework with processes for Web application security**

Vulnerabilities in Mobile Systems

- Risks from Remote Computing
  - the assumption that remote users are secure because they access the network via a VPN
  - Trusted Clients - are the clients who they say they are
  - Network Architecture - doesn't support remote computing
  - Policy Implementation - policies are incorrect, insufficient or weekly implemented
  - Stolen or lost devices
- Risks from Mobile Workers
  - Platform proliferation
    - Multiple devices used to access corporate network
  - Home based PC and multi-device synch solutions
    - Work information being backed up to home PC or the cloud

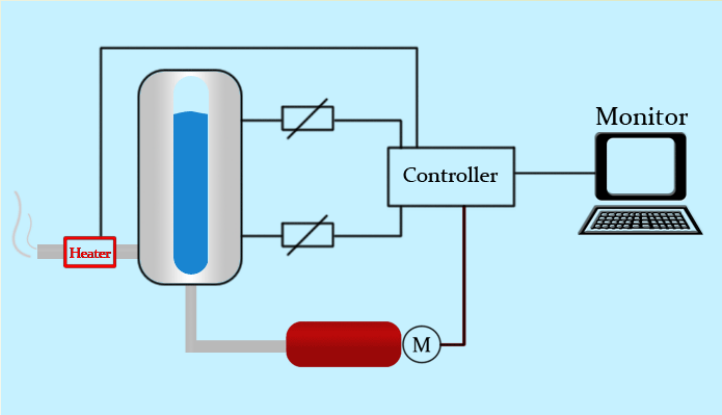
Mobile Targets

- SMS
- Email
- Phone
- Video/photo
- Social networking
- Location information
- Voice recording
- Documents
- Credentials

Embedded Devices and Cyber Physical Systems (CPS)

- **May have Universal Plug and Play (UPnP) access to networks**
- **CPS are smart networked systems with embedded sensors, processors, and actuators that are designed to sense and interact with the physical world.**
- **Where we find them:**
  - **Transportation, manufacturing, healthcare, energy, agriculture, defense, building controls, and emergency response systems**

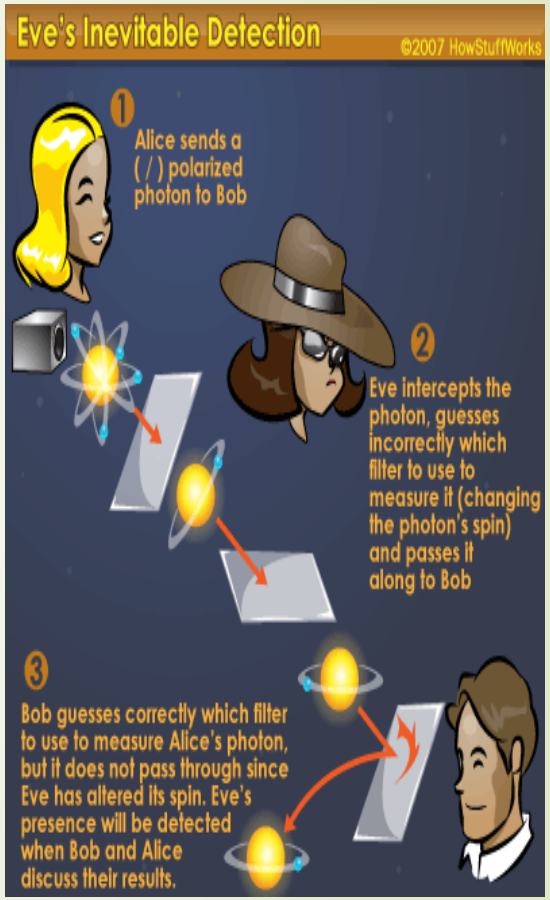
Industrial Control Systems (ICS)



- Based on standard embedded systems platforms
- Control industrial processes such as manufacturing, product handling, production, and distribution
- Well known ICS:
  - Supervisory Control and Data Acquisition (SCADA)
  - Distributed Control Systems (DCS)
  - Programmable Logic Controllers (PLC)

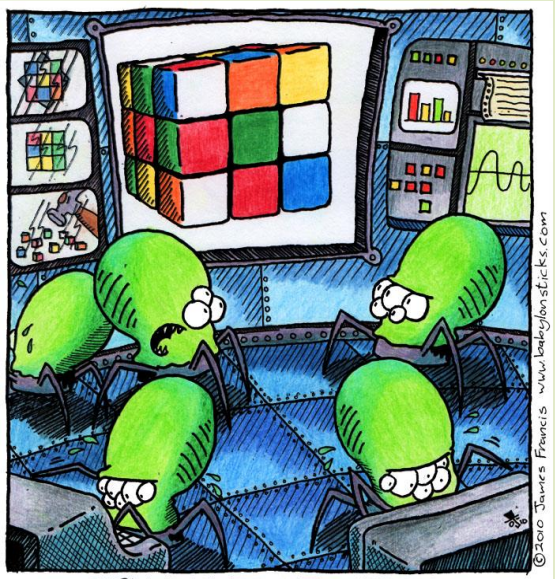
Quantum Cryptography

- Based on physics rather than mathematical difficulties
- Used for integrity and to generate/distribute secret keys
- Million times stronger than RSA in one millionth the time (uses qubit versus bit)
- Heisenberg Uncertainty Principle
  - In the process of measuring results, the results change
  - If photons intercepted, photons will change polarity



Cryptographic Services

- Confidentiality
- Integrity
- Availability (limited)
- Additional Services
  - Non-Repudiation
  - Authentication
  - Access Control
  - Data at Rest Protection
  - Data in Transit Protection
  - Link Encryption
  - End-to-End Encryption



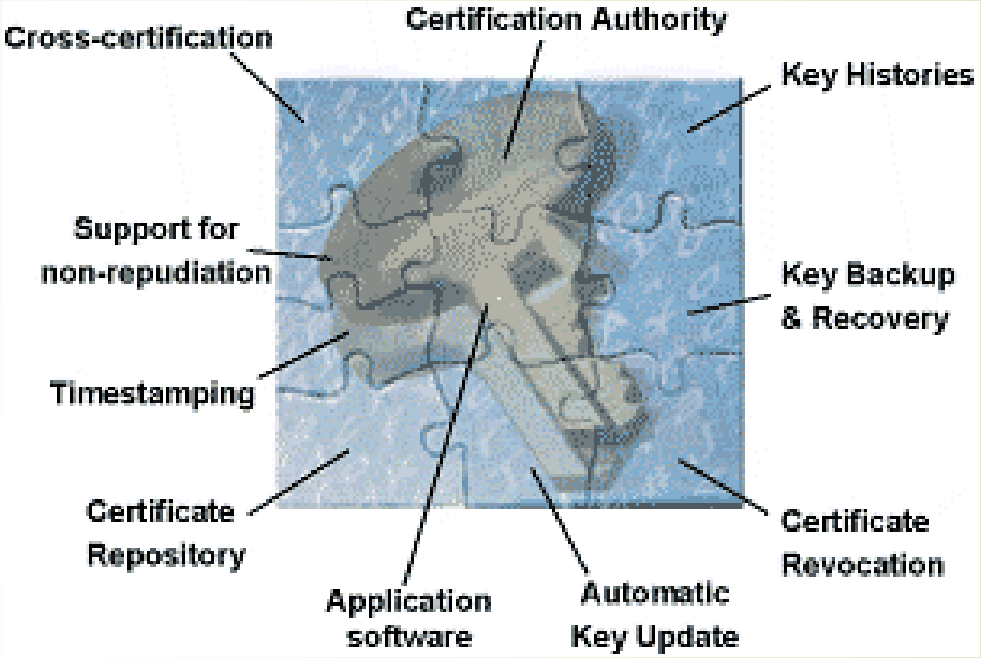
SIR! WE HAVE INTERCEPTED AN ADVANCED HUMAN ENCRYPTION DEVICE!

Public Key Infrastructure (PKI)

- Developed to provide a standards for:
  - Key generation
  - Authentication
  - Distribution
  - Storage of Asymmetric Keys

Key Management

- The process of
  - Setting policies
  - Protecting keys
  - Key recovery
  - Responding to key compromise
- Centralized Key Management
- Decentralized Key Management
- Key length: should be long enough to protect against attacks
- Cryptoperiod: key lifetimes (should be shorter for more critical data)



XML Key Management Specification 2.0 (XKMS)

- Defines the protocols for distributing and registering public keys
- Two parts:
  - XML Key Information Service Specification (X-KISS)
  - XML Key Registration Service Specification (X-KRSS)

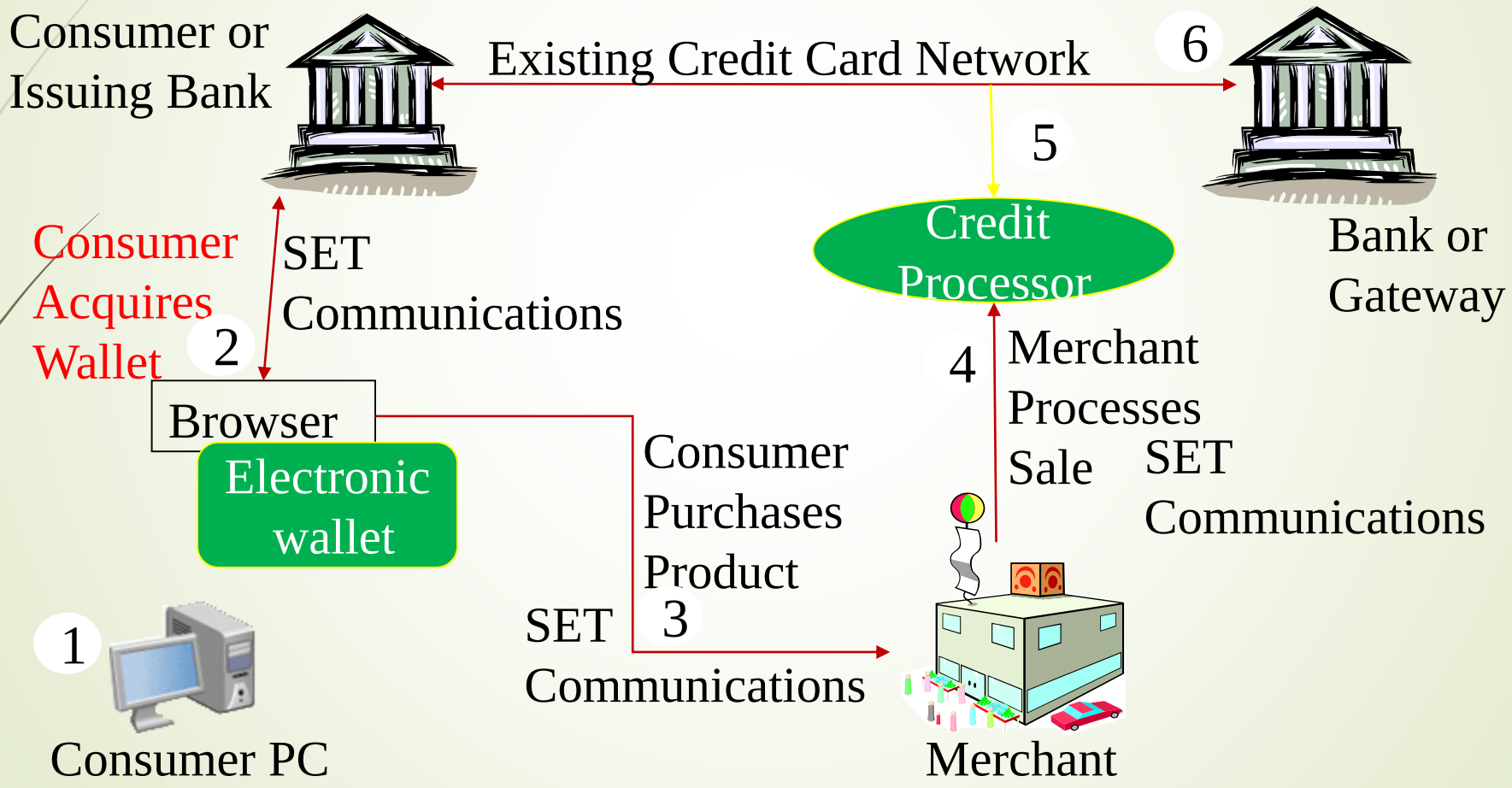
Standards for Financial Institutions

- ANSI X9.17 (American National Standards Institute)
  - Addresses the need to transmit securities and funds security over a electronic medium
  - Base on the hierarchy of keys
  - Data keys (DK)
    - Used to encrypt and decrypt messages with normally a single connection or message life span
- Master Key Encrypting Keys (KKM)
  - Must be distributed manually (Longer lifespan)
  - Two tier model (they encrypt the data keys)
  - Three tier model (they encrypt other key encrypting keys (KK) which are exchanged electronically and used to encrypt the data keys)

Key Wrapping and Key Encrypting Keys (KEK)

- Special purpose long term use key for key distribution or key exchange
- The process of using a KEK to protect a session key is called “key wrapping”
- Key wrapping can use either symmetric or asymmetric ciphers
- Used by SSL, PGP, S/MIME to provide session key confidentiality, integrity and sometimes authentication

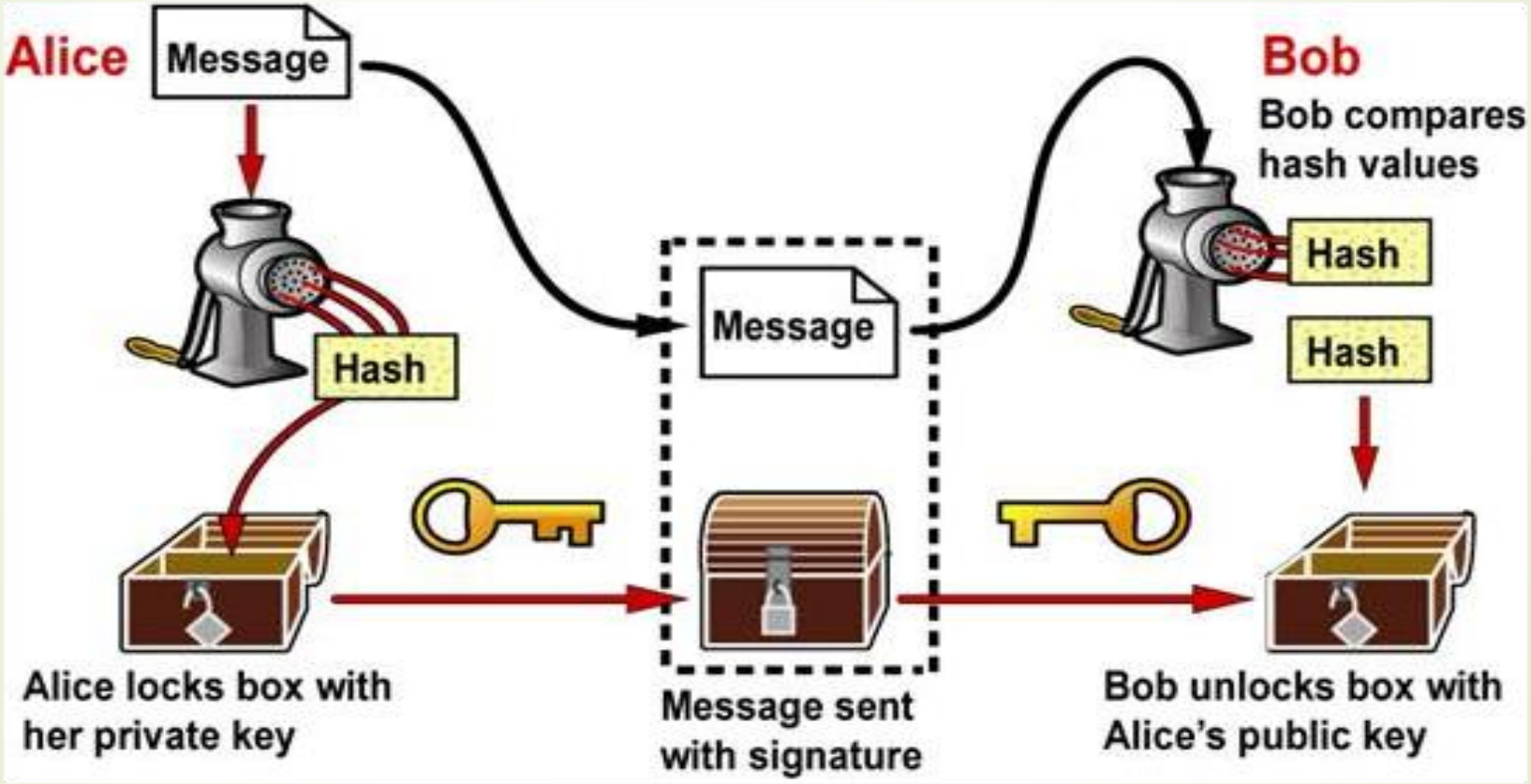
Secure Electronic Transaction (SET)



Key Management

- Key Storage
  - SW Based
  - HW Based
- Escrow
- Archival
- Recovery Agent
- Multiple Key Pairs

Digital Signing



Digital Signatures

- Used to authenticate the identity of the sender of a message/document
- Easily transportable
- Cannot be imitated by something else
- Can be automatically time stamped
- Provides integrity by encrypting the hash value with the sender's private key (message digest)
  - Financial transactions
  - E-Commerce
  - E-Mails

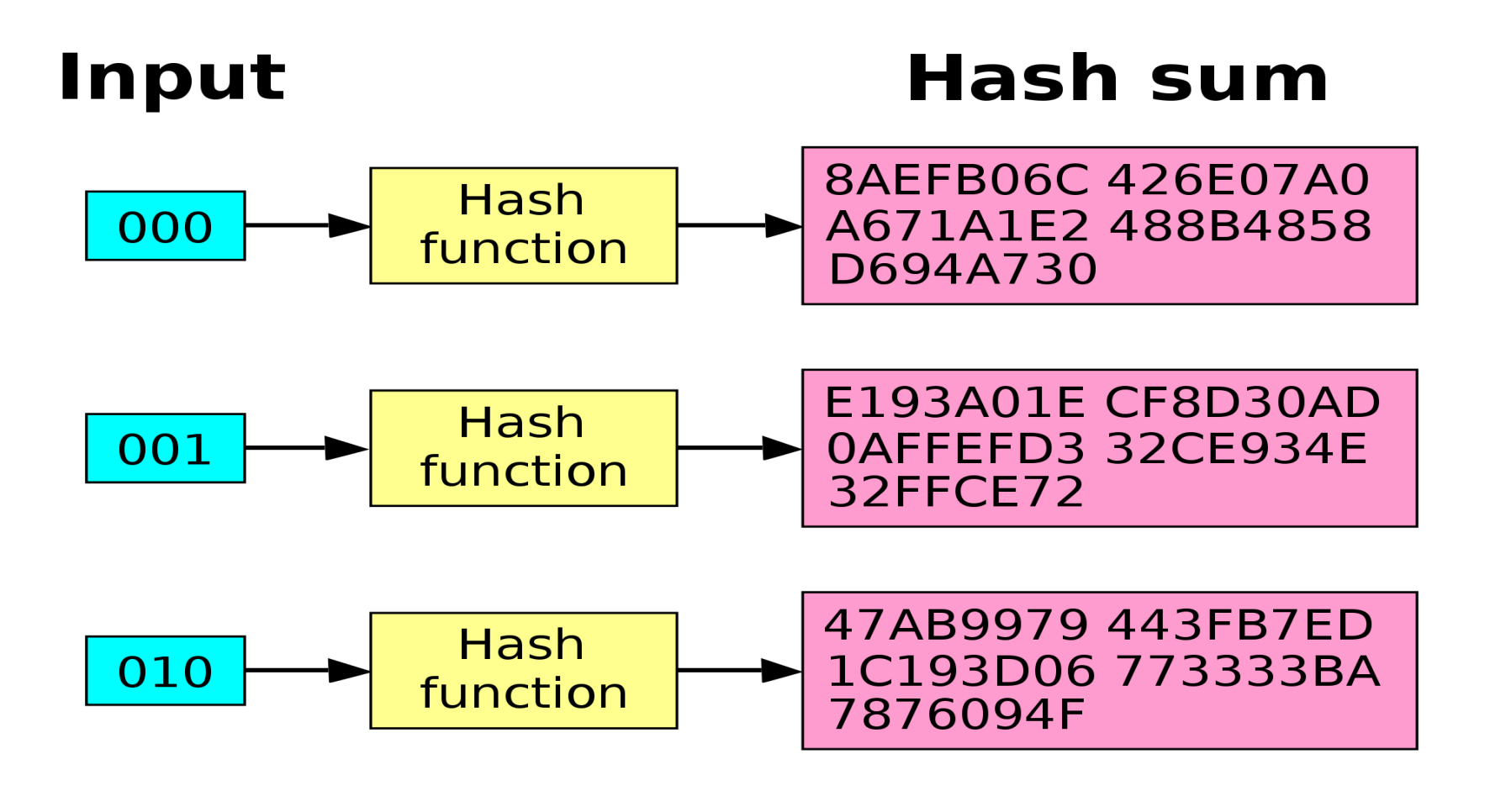
Digital Signature Standard

- Used to digitally sign documents
- U.S. Federal Government standard for digital signatures (FIPS 186)
- Performs integrity by use of SHA hashing
- Condenses the message to 160 bits
- Uses DSA, RSA, ECDSA

Digital Rights Management (DRM)

- DRM defines the interaction between the user, permissions, and content during the creation of content, distribution and upkeep of content, and use of content
- Lacks standardization
- 4 Types
  - Always on DRM
  - USB Key
  - Digital Watermark
  - Fingerprinting
- Amendment to copyright law known as the Digital Millennium Copyright Act (DMCA)

Hashing Algorithms - Avalanche Effect



Hashing Algorithms

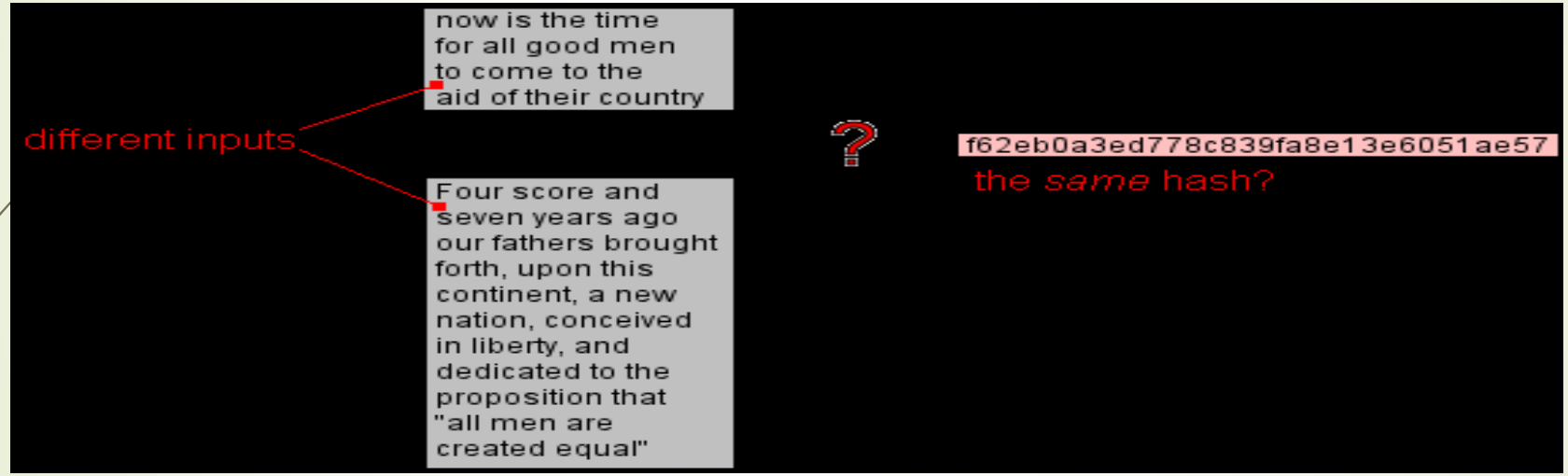
- A function that takes a variable-length string, and compresses and transforms it into a fixed-length
- The fixed-length output is called a hash or message digest
- Ensures data integrity
- Formula or method is public
- Used to create checksums, message digests, or integrity check values (ICV)

Hashing Algorithms

Name	Class	Hash Length
MD5	***512-bit blocks***	Digest size(s): **128 bits** Rounds: **4** **32 character output**
SHA-1,	***512-bit blocks***	Digest size(s): **160 bits** Rounds: **80** **40 character output**
SHA-2 SHA-224/256	***512-bit blocks***	Digest size(s): **256 bits** Rounds: **64** **56/64 character output**
SHA-2 SHA-384/512	**1024-bit blocks**	Digest size(s): **512 bits** Rounds: **80** **92/128 character output**
RIPEMD-160	***512-bit blocks***	Digest size(s): **160** Rounds: **5 paired rounds of 16 steps (160)**
HAVAL	**1024-bit blocks**	Digest size(s): **128 bits, 160 bits, 192 bits, 224 bits, and 256 bits** Rounds **3, 4, or 5**

Attacks on Hashing Algorithms

- **Collisions**



- **Brute-force: relies on finding weaknesses in the hashing algorithm**
- **Birthday Paradox: based on the probability with 23 individuals, 50% chance two of them will have the same birthday**

Cryptographic Attack Methods

- Ciphertext-Only
- Known-Plaintext (linear)
- Chosen-Plaintext (differential)
- Chosen-Ciphertext
- Differential Cryptoanalysis
- Linear Cryptoanalysis
- Known Key Attack
- Implementation Attacks
  - Side-Channel Analysis
  - Fault Analysis
  - Probing Attacks
- Analytic Attack
- Statistical Attack

Cryptographic Attack Methods

- Replay Attacks
- Algebraic
- Rainbow Table
- Frequency Analysis
- Factoring Attack
- Social Engineering for Key Discovery
- Dictionary Attack
- Reverse Engineering
- Random Number Generator Attacks
- Temporary Files

Other Attacks

- Meet-in-the-middle (against 3DES w/2 keys)
  - Encrypts the plaintext using all possible keys and creates a table with all possible results
  - Compares the results in the middle with the decryption of the corresponding ciphertext and each possible key
- Man-in-the-middle
  - Attacker sits between two communicating parties and intercepts all communications
  - Intercepts messages and forwards modified versions of the original message (aka Bucket Brigade attack)

Site Security

- Key Areas of knowledge
  - Site and facility design considerations
  - The protection and securing equipment
- Support the implementation and operation of:
  - Perimeter security
  - Interior security
  - Operations/facility security

Facility

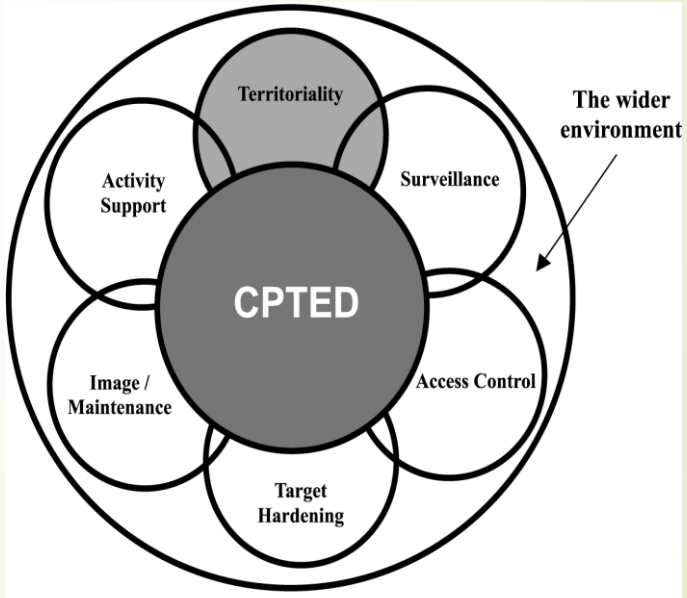
- Visibility
- Surrounding area and external entities
- Accessibility
- Natural Disasters
- Facility Design

Roadway Design for Facility Access

- Design strategies meant to:
  - Curtail unauthorized access
  - Prevent sabotage
  - Prevent structural damage
  - Minimize vehicle velocity

Crime Prevention Through Environmental Design (CPTED)

- Outlines how the proper design of a physical environment can reduce crime by affecting human behavior
  - Natural Access Control
  - Natural Surveillance
  - Territorial Reinforcement



Source: Adapted from Moffat (1983, p. 23)

Doors and Windows

- Door Design and Materials
  - Fail-secure
  - Fail-safe
  - Fail-soft

- Window Glass and Types
  - Standard
  - Tempered
- Reflective or shatter-proof security film
- Wire mesh or polycarbonate (embedded)
- Laminated (street level windows/doorways-2sheets of glass bonded to middle layer of resilient plastic)
- Acrylics
- Bullet resistant (1.25” thick resistant to 9mm round)

Glass Break Sensors

- Use both acoustic and shock wave sensors for maximum effectiveness (dual alarm system)
  - This reduces false positives
- Acoustic sensors
  - Listen for sound of breaking glass
- Shock wave sensors
  - Feel the shock wave when the glass is broken

WALLS

- Wall thickness protections
  - ½ inch gypsum, wood studs, fiber insulation give you 1 hour of fire protection.
  - The rule of thumb is one inch of gypsum = 1hour of protection
- Fire standard calls for computer rooms to be separated by fire resistant walls, floor, ceiling constructed of noncombustible or limited combustible materials, rated at not less than one hour (Passive Fire Protection)

Fire Prevention, Detection and Suppression

- Fire (heat), flame, and smoke detection systems
  - Ionization (smoke)
  - Heat
    - Rate of Rise
    - Fixed Temperature
  - Photoelectric (Smoke)
- Ultraviolet/Infrared (flame)
- Fire Suppression
  - Fire suppression devices
  - Fire suppression methods

Fire Suppression Devices

Class	Type	Suppression Material
A	Common Combustible (paper, wood, cardboard, most plastics)	Water, foam
B	Liquids (gasoline, kerosene, grease, oil)	CO_2, Halon, foam and dry powder
C	Electrical (electrical appliances, wiring, circuit breakers)	CO_2, Halon, dry powder (never use water)
D	Metal (found in chemical laboratories: magnesium, titanium, potassium, sodium)	Dry Powder
K	Kitchen Fires	Wet Chemicals

Fire Suppression Methods

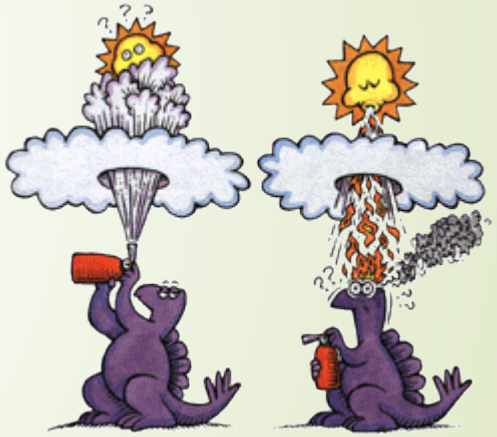
- Water
  - Wet Pipe
  - Dry pipe
  - Preaction
  - Deluge
- Gas
  - CO2
  - Halon
  - Aero-K
- Powder
- Foam

Suppression methods	How suppression works
Soda acid	Removes fuel
Carbon Dioxide	Removes O_2
Water	Reduces temperature
Gas	Interferes with the chemical reactions between elements

Fire Suppression Methods

Montreal Protocol on substances that deplete the ozone layer (1989)

- **Halon Replacements:**
  - **FM-200**
  - **INERGEN**
  - **CEA-308**
  - **CEA-410**
- **NAF-S-III**
- **FE-13**
- **ARGON**
- **ARGONITE**



Utility Concerns

- Electrical
  - Guarantee essential power to facility services required for daily operations and life safety
- Communications
  - Is an integral part of the core facility utilities
- Utilities
  - May suffer damage when subjected to the shock of extensive environmental hazards
  - May be critical for the safety of the facility

Communications and Server Rooms

- Located in core area of facility
- Not directly accessible from public areas
- Should not be located on top floors or basements, but should be located well above the ground floor.
- Placed on different electrical grid from rest of facility
- Need higher level of security
- Rack security (rack locks)

Restricted Work Area Security

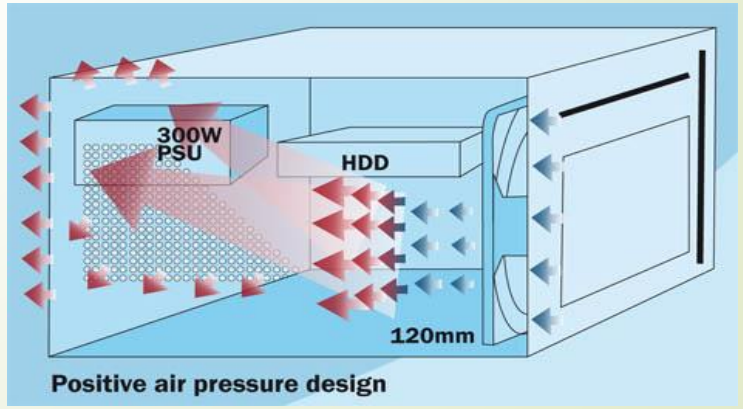
- Store sensitive information in containers (lockable filing cabinet)
- Clean desk approach
- Strong passwords for workstations
- Face computer screens away from windows
- Have a shredder available
- Highly restricted areas (i.e. SCIF) require more security to ensure tighter access control

Data Center Security

- Segregated from access areas
- Access based on “need to know”
- Security in depth starting from least sensitive to most sensitive
- Combining different methods of access control at different areas increases security at inner levels
- Internal mantraps provide increased entry and exit control
- Two person rule requires at least one other person in the room or area for access

Utilities and HVAC Considerations

- Electric Power
  - Power Protection
    - Complete loss of power
    - Degradation of power
    - Excess of power
- Environmental Issues
  - Positive drains
- Ventilation
  - Positive pressure
  - Closed-loop recirculation



Utilities and HVAC Considerations

- Power and Electricity
  - Inrush: Initial surge after connection to power
  - Noise: Steady interference
    - EMI (ElectroMagnetic Interference)
    - RFI (Radio Frequency Interference)
  - Transient: Short duration interference
  - Clean: Non-fluctuating power
  - Ground: The wire in an electrical circuit that is grounded

Utilities and HVAC Considerations

- Temperature, Humidity, and Static
  - Temperature
  - 60 to 75 °F (15 to 23 °C)
  - Humidity level
  - 40 to 60 %
  - Static electricity
- Water
  - Water leakage
  - Flooding
  - Positive drains

Material or Component	Damaging Temperature
Computer systems and peripheral devices	175 °F
Magnetic storage devices	100 °F
Paper products	350 °F

Education, Training and Awareness

- Number one goal of physical security is personnel safety
- Physical and procedural security requirements should never put anyone at risk
- Evacuation routes should be posted with quickest exits identified.
- Special care should be given to deal with handicapped personnel (Reserve use of elevators to handicapped)
- Meeting points should be identified where evacuated personnel can gather
- Two primary evacuation roles exist:
  - Safety warden
  - Meeting point leader

Questions?

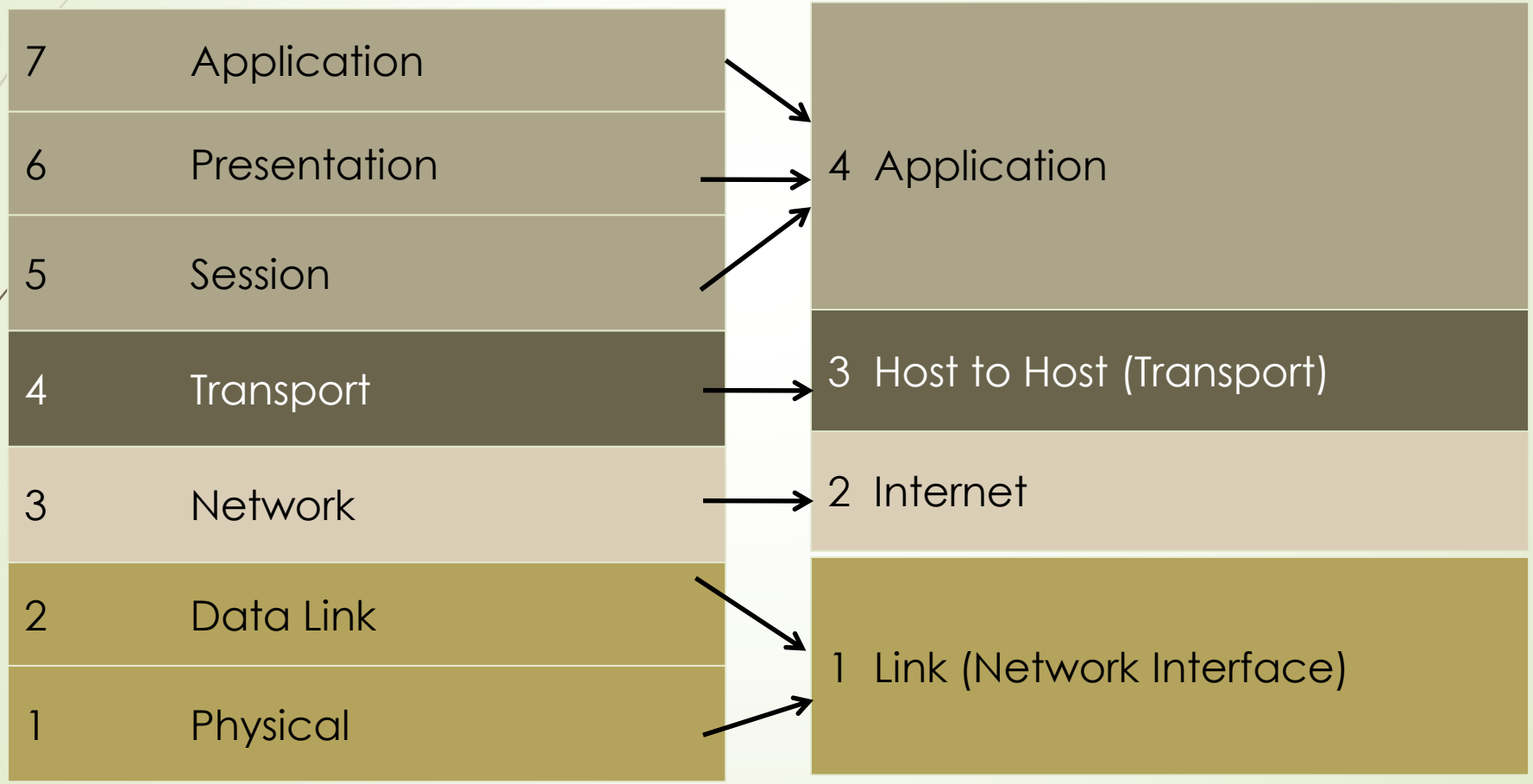
Communications and Network Security

(Designing and Protecting Network Security)

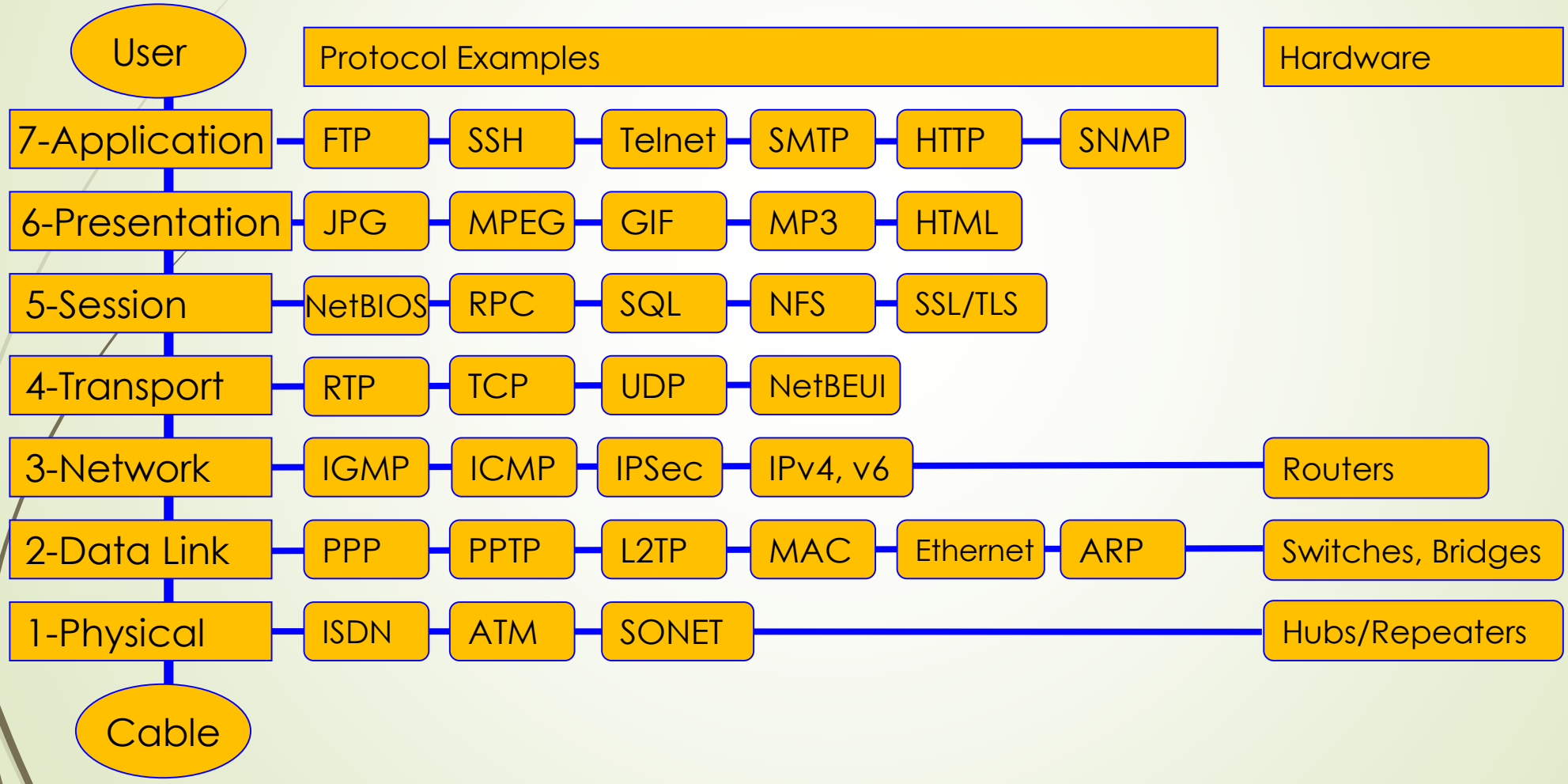
Domain Objectives

- Apply secure design principles to network architecture
- Actively secure network components
- Design and establish secure communications channels
- Prevent or mitigate network attacks

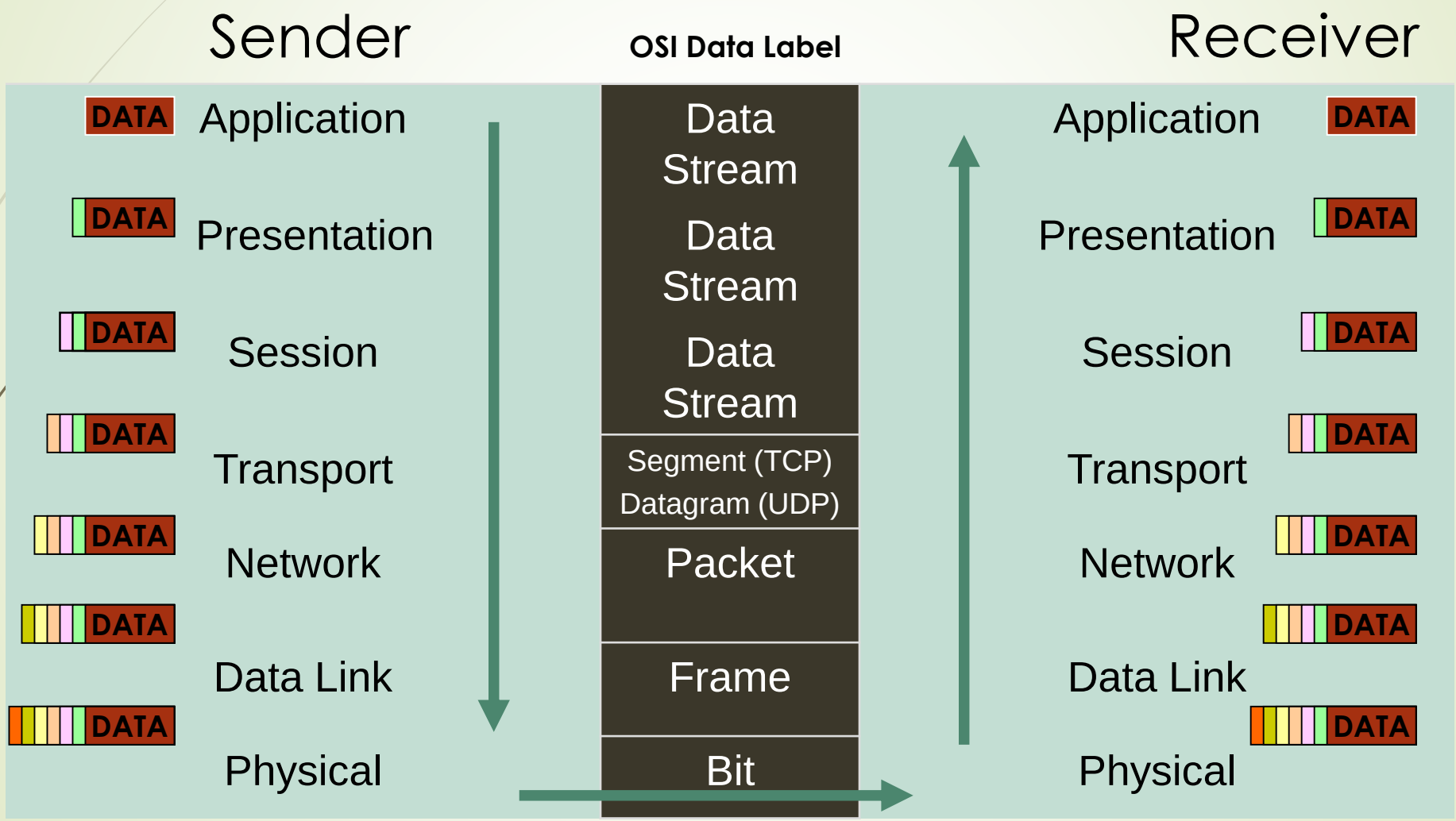
Secure Network Architecture & Design - OSI & TCP/IP Models



Secure Network Architecture & Design - OSI Model Overview



Data Encapsulation / De-encapsulation

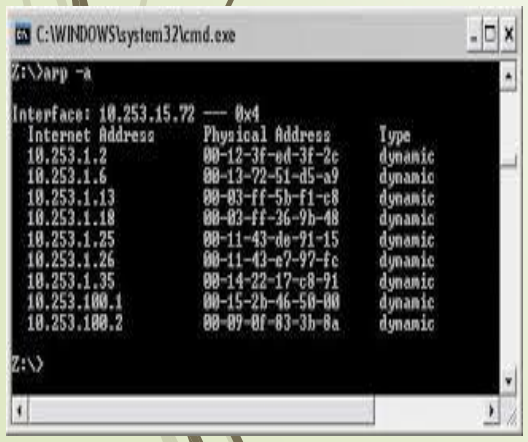


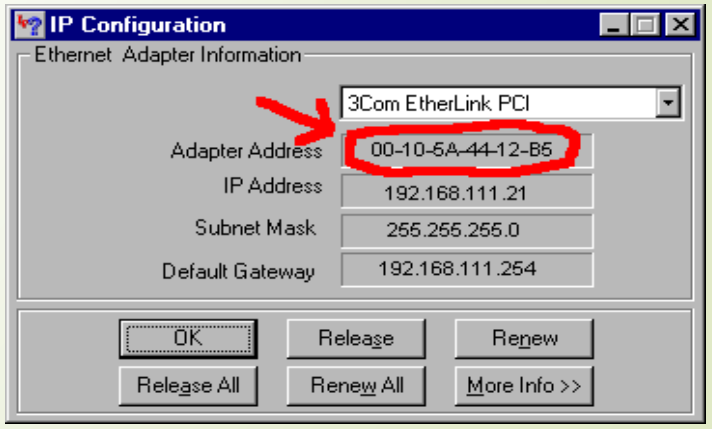
Secure Network Architecture & Design - OSI Model Overview

- Layer 1: Physical Layer
  - Responsibilities:
    - Definition of HW Specifications
    - Encoding and Signaling
    - Data Transmission and Reception
    - Topology and Physical Network Design

Secure Network Architecture & Design - OSI Model Overview

- Layer 2: Data Link Layer
  - Key tasks performed:
    - Logical Link Control (LLC)
    - Media Access Control (MAC)
    - Data Framing
    - Addressing
      - MAC
      - EUI-64 MAC
    - Error Detection and Handling
    - Protocols
      - ARP
      - RARP



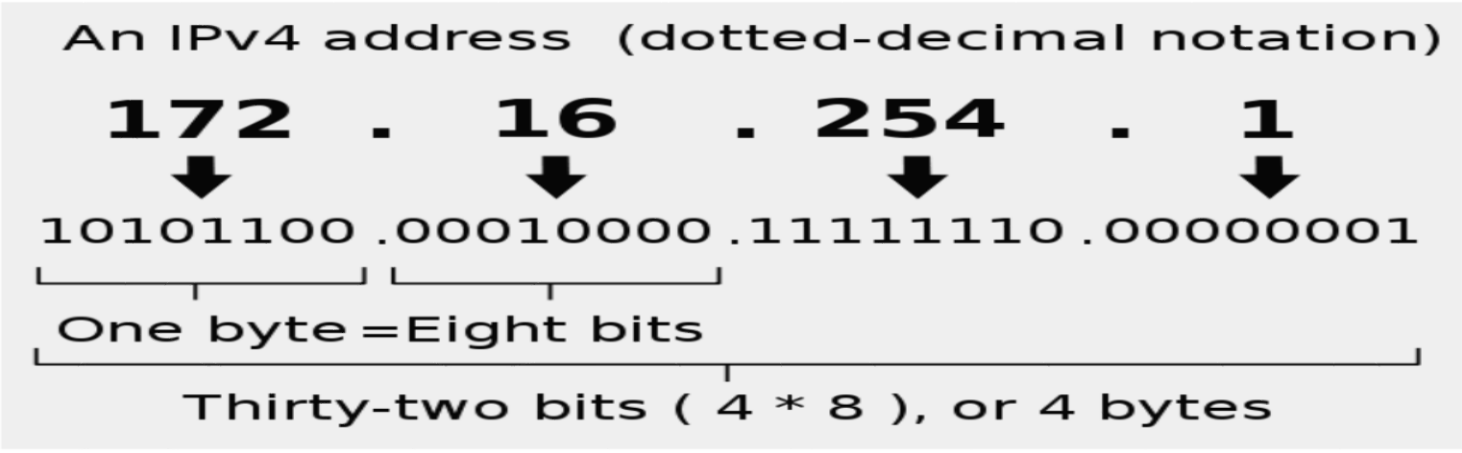


Secure Network Architecture & Design - OSI Model Overview

- Layer 3: Network Layer
  - **Key tasks performed:**
    - Logical Addressing
      - Internet Protocol Version 4 (IPv4)
      - Internet Protocol Version 6 (IPv6)
    - Routing
    - Datagram Encapsulation
    - Fragmentation Reassembly
    - Error Handling and Diagnostics
- Protocols
  - Internet Protocol (IP)
  - Internet Control Management Protocol (ICMP)
  - Internet Group Management Protocol (IGMP)

Layer 3: Network Layer - Internet Protocol Version 4 (IPv4)

- IPv4 (32-bit)
  - Can you list all the IPv4 Class ranges?
  - CIDR Notation
  - 158.6.12.1/22 = 22 Network bits, 10 host bits
  - 78.45.23.2/12 = 12 Network bits, ___ host bits



Layer 3: Network Layer - RFC 1918

- Sets aside addresses for internal use only
- Addresses not routable on Internet
- Often associated with NAT (Network Address Translation) scenarios

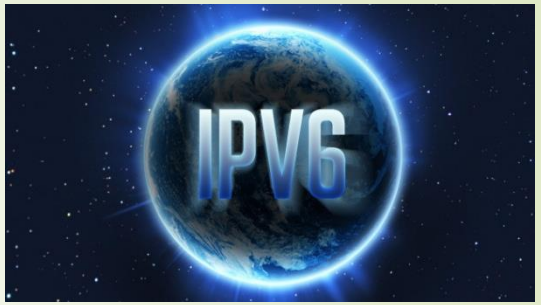
Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

Layer 3: Network Layer - Internet Protocol Version 6 (IPv6)

- Written in hexadecimal, with pairs of bytes separated by colons
  - Pairs of bytes are referred to as blocks
  - Hexadecimal digits, or half-bytes are called nibbles

- Sample address:
  - Fe80:0000:0000:0000:002c:ff1f:ffed:db2e
- Same address abbreviated using zero compression:
  - Fe80::2c:ff1f:ffed:db2e
- A double-colon can be used to represent all contiguous blocks of zeros
  - You can only use the double-colon once per address
- Loop back address:
  - 0000:0000:0000:0000:0000:0000:0000:0001 or ::1

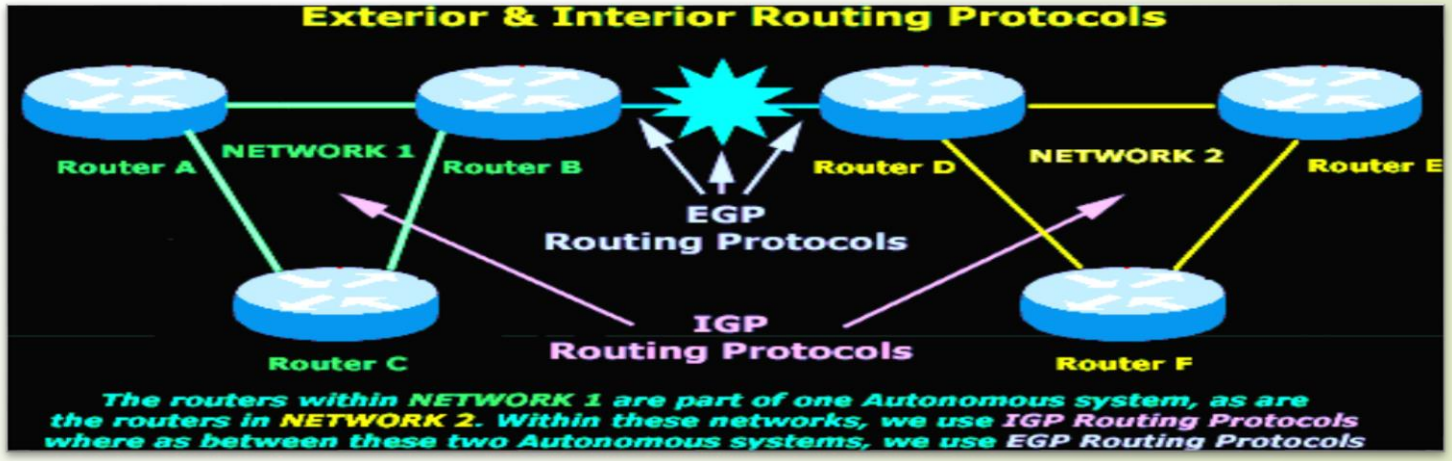
Layer 3: Network Layer – IPv6



- Link-local scope:
  - Not routed. Only used within a single subnet
  - will automatically acquire a link-local address starting with a prefex of fe80::/64
- Site-local scope:
  - Address only routed within a “site” (nodes not reachable by the Internet)
  - Three prefixes exist for site-scoped unicast addresses
- Global scope:
  - Addresses routed throughout the entire Internet
- Multicast Addresses
  - Used for internal purposes
  - Multicast addresses start with the ff00::/8 prefix (last 7 blocks make up the multicast group ID)

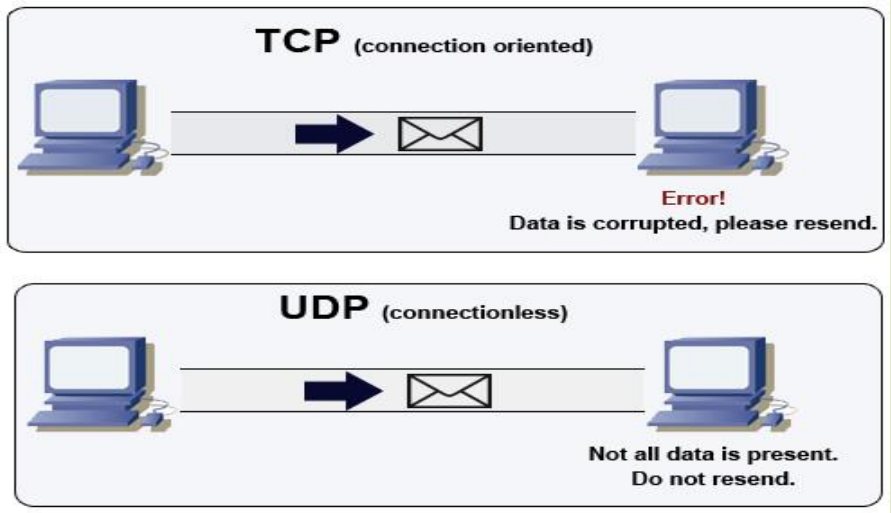
Layer 3: Network Layer - Routers

- Routers (forward packets onto logical routes)
  - Separate subnetwork broadcasts (and collisions)
  - Diverse routing
  - Distance-vector
  - Link-state
  - Convergence
- Routing Protocols
- Interior Gateway Protocols
  - RIP/RIPv2
  - OSPF
- Exterior Gateway Protocols
  - BGP



Secure Network Architecture & Design - OSI Model Overview

- Layer 4: Transport Layer
  - Services
    - Keeps track of what data comes from each application
    - Defines the means by which large amounts of application data are divided into smaller blocks for transmission
- Quality
- Ensures that data are received as sent



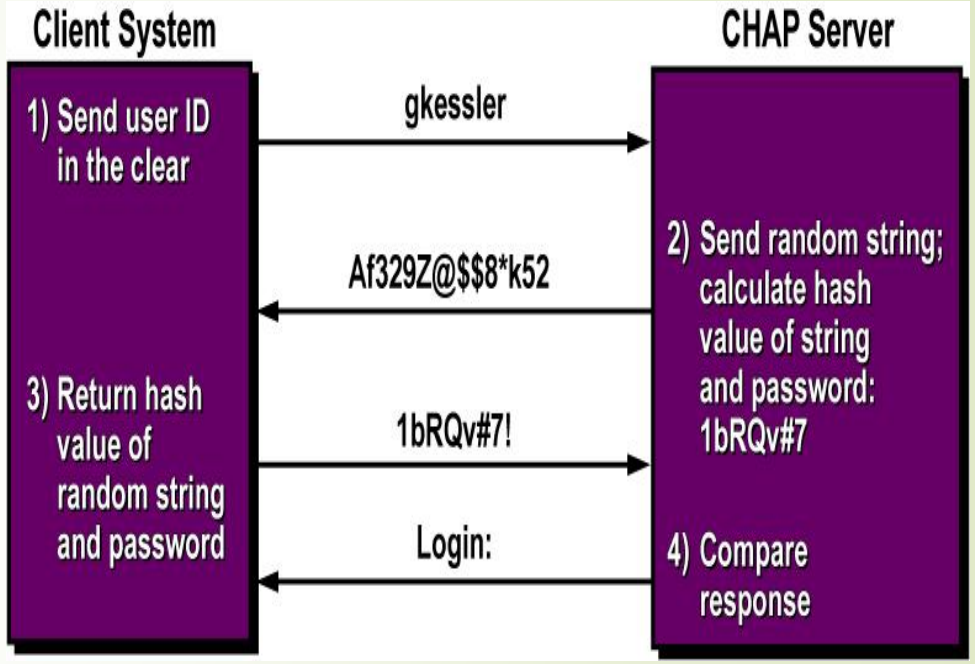
Secure Network Architecture & Design - OSI Model Overview

- Layer 5: Session Layer
  - Primary function
    - Provide the means necessary to set up, manage, and end sessions
    - 3 modes
      - Full-Duplex
      - Half-Duplex
      - Simplex
    - Uses command sets called Application Programming Interfaces (APIs)
      - Allows an application to accomplish certain high level communications over the network
      - Common APIs
        - NetBIOS
        - TCP/IP Sockets
        - Remote Procedure Calls (RPCs)

Layer 5: Session Layer - PAP & CHAP

- Password Authentication Protocol (PAP)
  - Password traverses network in the clear
  - Susceptible to replay attacks

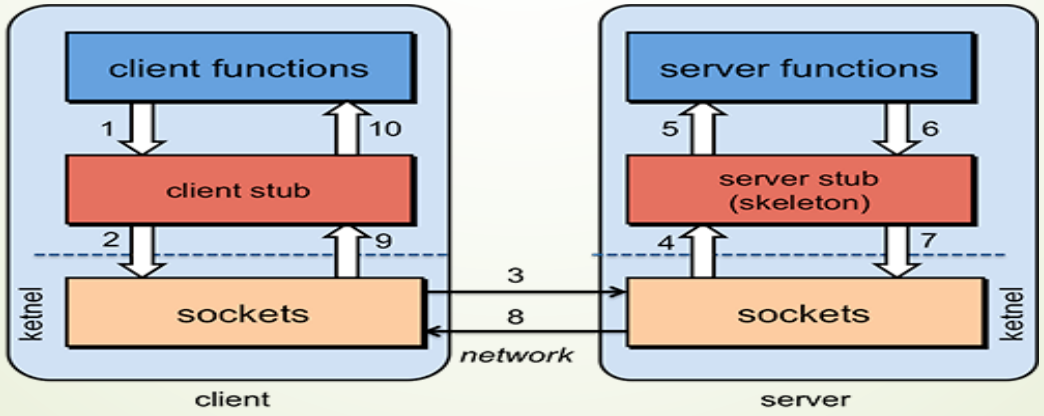
- Challenge Handshake Authentication Protocol
  - Provides centralized authentication
  - Passwords not exposed to network
  - Provides protection against replay attacks
    - Periodically challenges for a new authentication exchange
  - Authenticates in one direction but can be used for mutual authentication



Layer 5: Session Layer - Remote Procedure Calls (RPC)

- **Creates the ability for a client to send instructions to an application residing on another system.**

- **RPC does not provide any services but instead brokers service by providing authentication and a way to contact the actual service.**



Secure Network Architecture & Design - OSI Model Overview

- Layer 6: Presentation Layer
  - Architecture includes:
    - Functions:
      - Translation
      - Compression
      - Encryption and Decryption
    - 2 Sublayers:
      - Common Application Service Element Sublayer (CASE)
      - Specific Application Service Element (SASE)

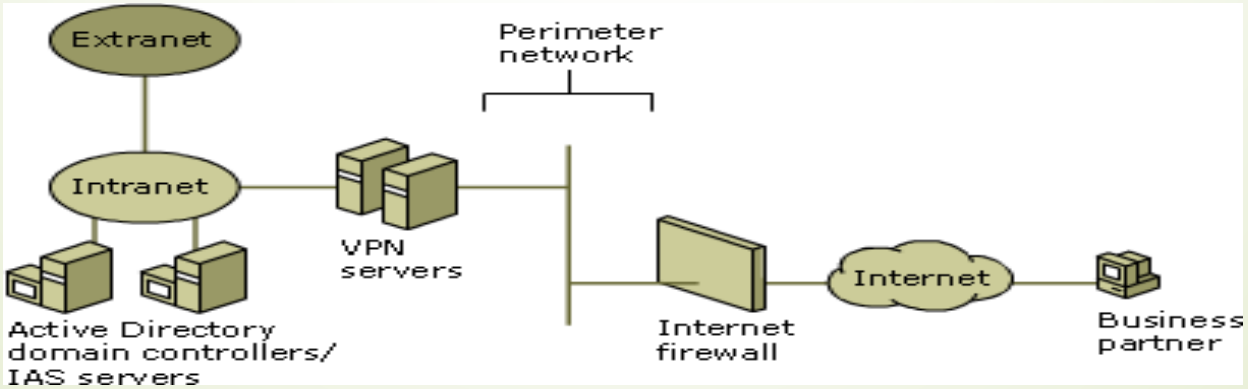
Secure Network Architecture & Design - OSI Model Overview

- Layer 7: Application Layer
  - **Is used by network applications**
  - **Provides services for user applications to employ**
  - **Implements the functions that are needed by users of the network**

Secure Network Architecture & Design - Intranet & Extranet

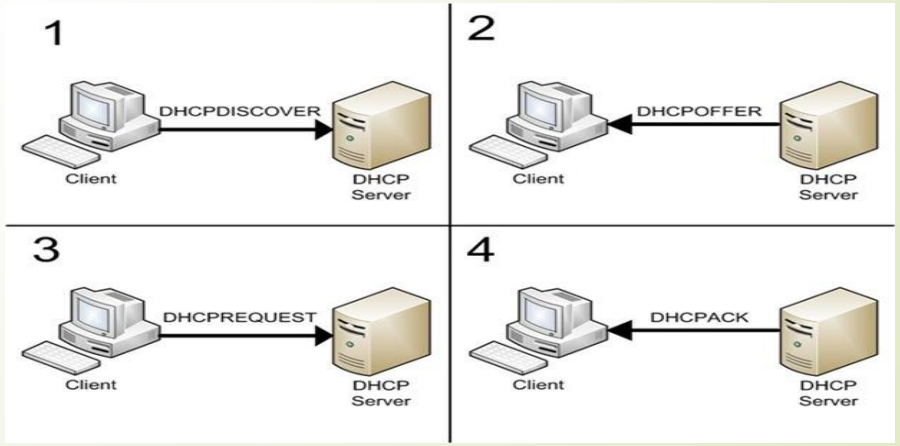
- **Intranet:**
  - **Network of interconnected internal networks within an organization, which allows information to be shared within the organization**

- **Extranet:**
  - **To be more competitive, companies share information with their business partners and provide nominally proprietary account information to clients**



Secure Network Architecture & Design - Dynamic Host Configuration Protocol (DHCP)

- **Automatically assigns IP addresses to workstations**
- **Designed to replace BOOTP (bootstrap protocol) which would determine the IP address, OS, and download the operating system via TFTP**
- **UDP port 67 for servers**
- **UDP port 68 for clients**



Secure Network Architecture & Design - Directory Services

- **Hierarchy of objects storing info about users, groups, systems, servers, printer, etc.**

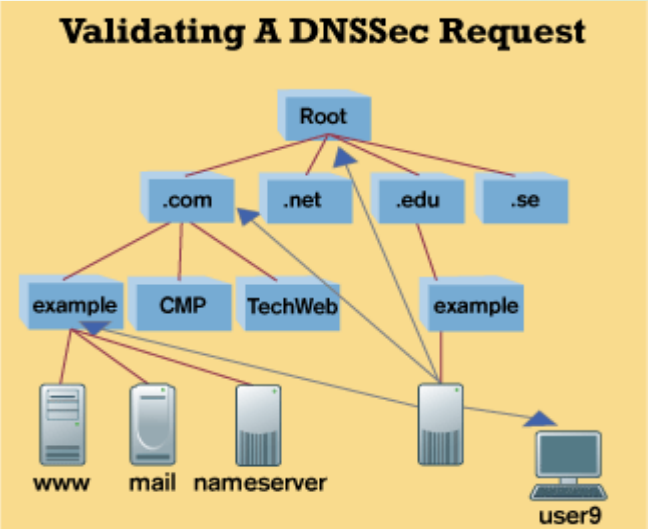
- **Examples:**
  - **Lightweight Directory Access Protocol**
  - **Active Directory**

Secure Network Architecture & Design – Directory Services

- Domain Name System (DNS)
  - An IETF standard naming system for resources connecting to the internet
  - Translates domain names to IP addresses
  - TCP / UDP 53
  - Authoritative name servers provide resolutions for a given domain
- DNS Weaknesses
  - UDP is unreliable
  - Domain Kiting
  - DNS Spoofing/DNS Cache Poisoning
  - Social Engineering
  - Information disclosure
  - Name space related risks
  - DNS Amplification Attacks

Secure Network Architecture & Design – Directory Services

- Domain Name Server Security Extensions (DNSSEC)
  - Provides integrity and authentication for DNS responses
  - Uses PKI (digital signatures)
  - Implementation is ongoing



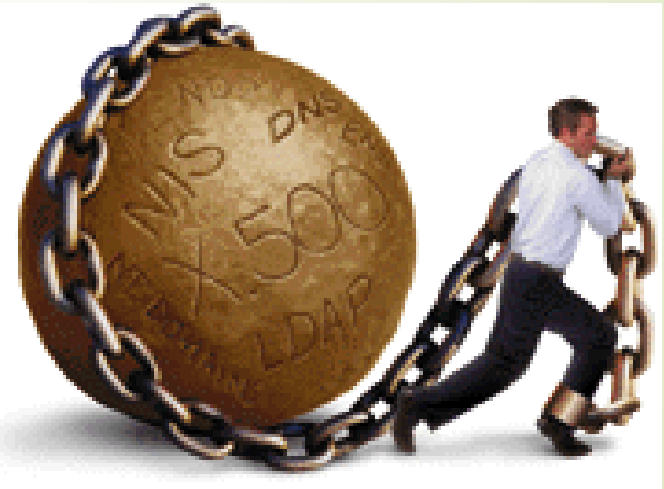
Root signs the .com, .net, .edu, and other TLD (top-level domain) records. The .com domain then signs all of its delegated zones. Example signs records for hosts under it. When user9 tries to resolve *www.example.com*, its nameserver walks down the DNS tree as normal, but also validates responses at each step. If no problems are detected, nameserver sends a response to user9. Optionally, user9 could request all DNSSec records and do its own validation.

Secure Network Architecture & Design – Directory Services

- **Network Basic Input/Output System (NetBIOS)**
  - **NetBIOS was developed in the early 1980s to allow applications to communicate over a network.**
  - **NetBIOS services should be disabled on servers (Ports 135, 137, 138, and 139) or a firewall is in place between server and internet**

Secure Network Architecture & Design – Directory Services

- Network Information Service (NIS+)
  - Developed by Sun Microsystems to centralize the administration of Unix systems
  - Managing user credentials across a group of machines
  - Flat name space called domains.
  - NIS Weakness:
    - Potential spoofing
  - NIS+ (more secure)



Secure Network Architecture & Design – Directory Services

- File Sharing
  - Technology and implementation
    - Access services
      - Common Internet File System (CIFS) / Server Message Block (SMB)
      - NFS
      - SNFS
        - NFS v.4 protocol

Secure Network Architecture & Design – Directory Services

- Email Protocols
  - Server email protocol
    - Simple Mail Transfer Protocol (SMTP)
      - Protocol to route email on the Internet
      - TCP 25 & SMTPS – port 465
    - Enhanced Simple Mail Transfer Protocol
      - Addresses weaknesses in SMTP
- Client email protocols
  - Post Office Protocol (POP3)
    - TCP 110 (POP3) & POP3S – port 995
  - Internet Message Access Protocol (IMAP4)
    - TCP 143 & IMAPS – port 993

Secure Network Architecture & Design – Directory Services

- Secure Shell (SSH)
  - Secures remote terminal communications
  - Secure replacement for Telnet, FTP, and Unix r-commands
  - Protects against sniffing, spoofing, and man-in-the-middle attacks
  - Encrypts data using symmetric algorithms
  - Establishes connection and authentication using public key cryptography
  - Uses TCP port 22
  - Only use SSH version 2 as version 1 is vulnerable to MITM attacks

- Contains: ssh, sftp, scp, slogin

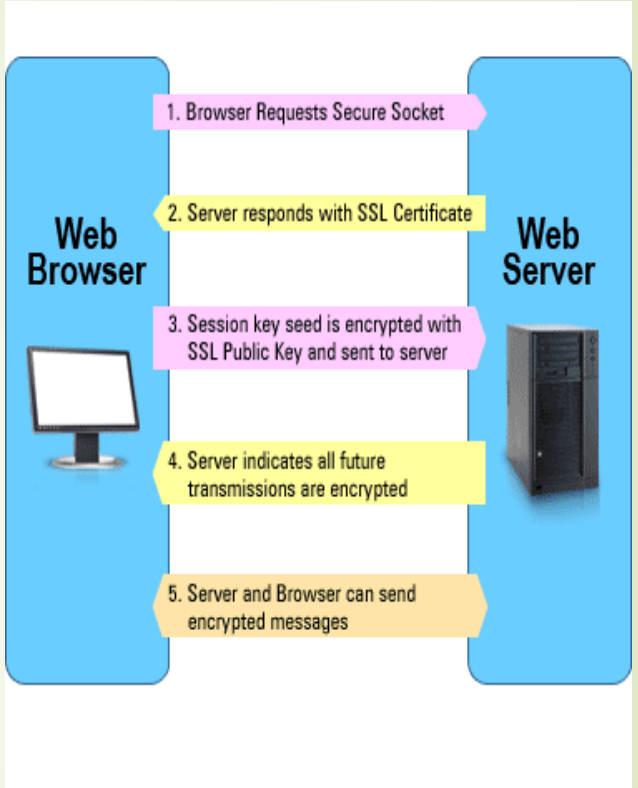
Secure Network Architecture & Design – Directory Services

- Data Exchange and Transfer Protocols
  - File Transfer Protocol
    - TCP port 20 (data stream) /21 (control stream)
    - Transfer modes
      - Active
      - Passive

  - Trivial FTP (TFTP)
    - UDP port 69
    - No authentication or directory structure
    - No confidentiality or integrity

Secure Network Architecture & Design – Directory Services

- HTTP/HTTPS/S-HTTP
  - HyperText Transfer Protocol (HTTP)
  - HTTP Proxying
    - Anonymizing proxies
    - Open Proxy servers
    - Content filtering
    - HTTP Tunneling
- HTTPS (TCP 443)
- S-HTTP (TCP 80)
- Peer-to-peer
- Passive and active content (HTML, ActiveX, Java and JavaScript)

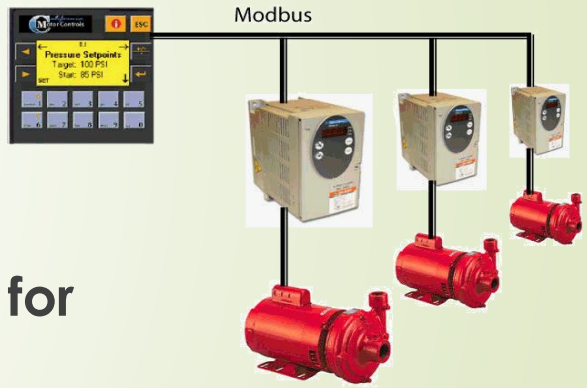


Implications of Multi-layer Protocols - SCADA (Supervisory Control and Data Acquisition)

- Most SCADA systems contain:
  - Control server
  - Remote Terminal Unit
  - Human machine interface
- Programmable logic controller
- Intelligent electronic devices
- Input/output server
- Data historian (central log)

Implications of Multi-layer Protocols - MODBUS/FIELDBUS

- **Communication protocols where the focus is uptime and control of devices**
- **Cleartext protocols**
- **Supported devices often use little to no authentication for command execution**
- **Require encapsulation or isolation from public/open networks**

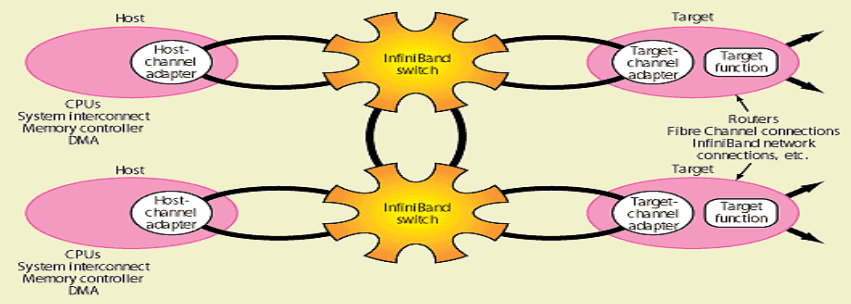


Converged Protocols - IP Convergence

- IP Convergence occurs as information and communications assets such as business data, voice-telephony, physical security controls, and industrial control systems migrate to IP
- IP Convergence makes the network event more sensitive to security events and makes the job of secure telecommunications even more vital
- Converged Networks:
  - InfiniBand
  - Internet SCSI
  - FC over IP
  - Internet FC Protocol

Converged Network: InfiniBand (IB)

- Converged network capability
- Transports Inter-processor communications, LAN, storage protocols
- Two most common storage protocols
  - SCSI Remote Direct Memory Access Protocol (SRP)
  - ISCSI Extensions for RDMA (iSER)



InfiniBand, a switch-fabric architecture, offers far greater bandwidth than the bus-structured architectures of the past. It also eases redundancy and hot-pluggability problems. This network approach segments 2-Gbyte messages into 256- to 4096-byte packets.

Converged Network: FC over IP (FCIP)/Internet FC Protocol (IFCP)

- Map Fibre Channel framing on top of TCP/IP
- SAN extension protocol for bridging SANs that geographically diverse
- Complex
- Expensive
- Lack of scalability

Converged Network: Data Center Bridging (DCB)Standards

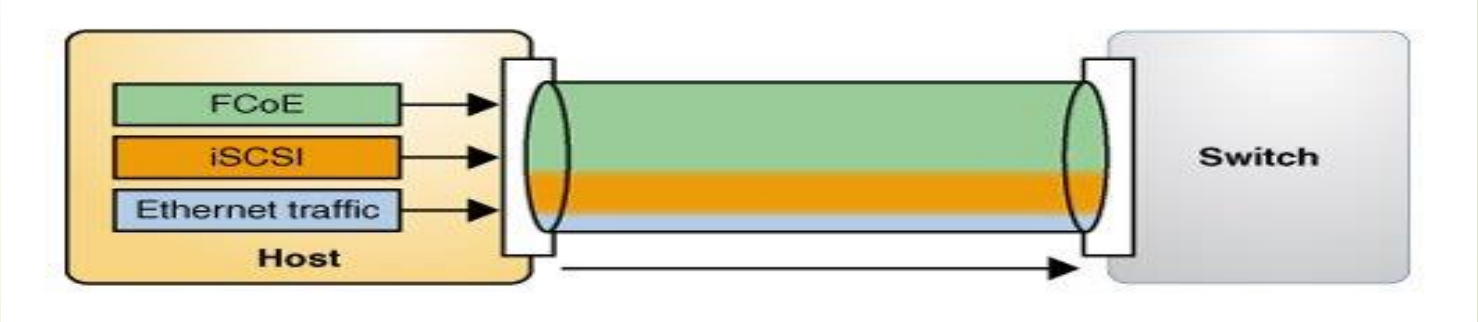
- Block storage protocols to be converged as 10GbE becomes more widespread
- Relies on the DCB standards which applies to any IEEE 802 network
- DCB defines 4 new technologies:
  - Priority-based Flow Control (PFC)
  - Enhanced Transmission Selection (ETS)
  - Quantized Congestion Notification (QCN)
  - Data Center Bridging Exchange Protocol (DCBX)

DCB Technology: Priority Based Flow Control (PFC)

- 802.1Qbb allows the network to pause network traffic
- Enables flow control for different network classes

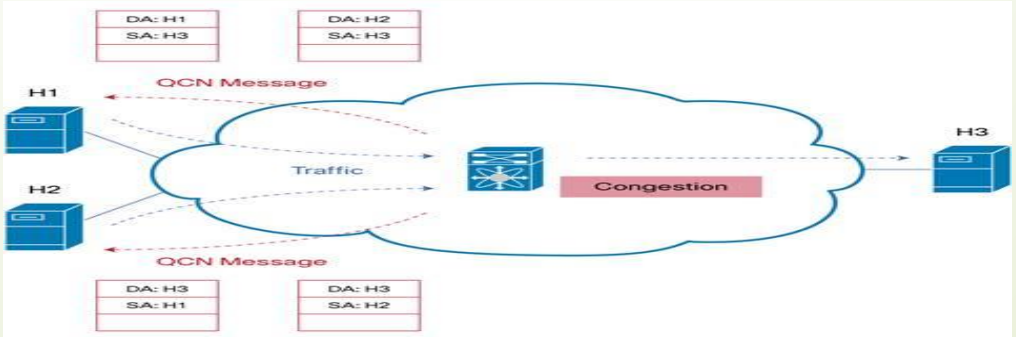
DCB Technology: Enhanced Transmission Selection (ETS)

- 802.1Qaz defines the scheduling behavior of multiple traffic classes
- Enables:
  - Fair sharing of the link
  - Better performance
  - Metering



DCB Technology: Quantized Congestion Notification (QCN)

- 802.1Qau supports end-to-end flow control in a switched LAN
- Eliminates sustained or heavy congestion in Ethernet networks
- Uses PFC to ensure a lossless environment and avoid dropping packets

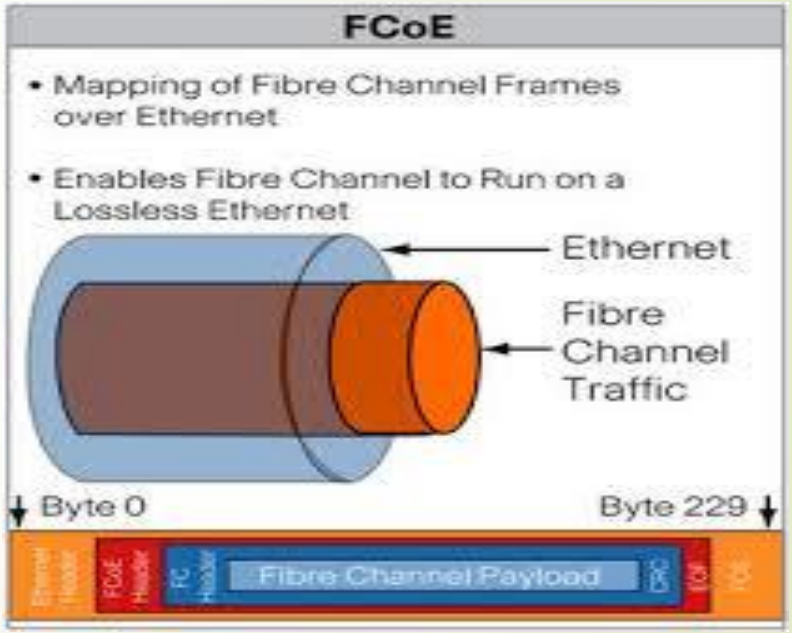


DCB Technology: Data Center Bridging Exchange Protocol (DCBX)

- 802.1Qaz supports discovery and configuration of network devices that support:
  - Priority Based Flow Control
  - Enhanced Transmission Selection
  - Quantized Congestion Notification

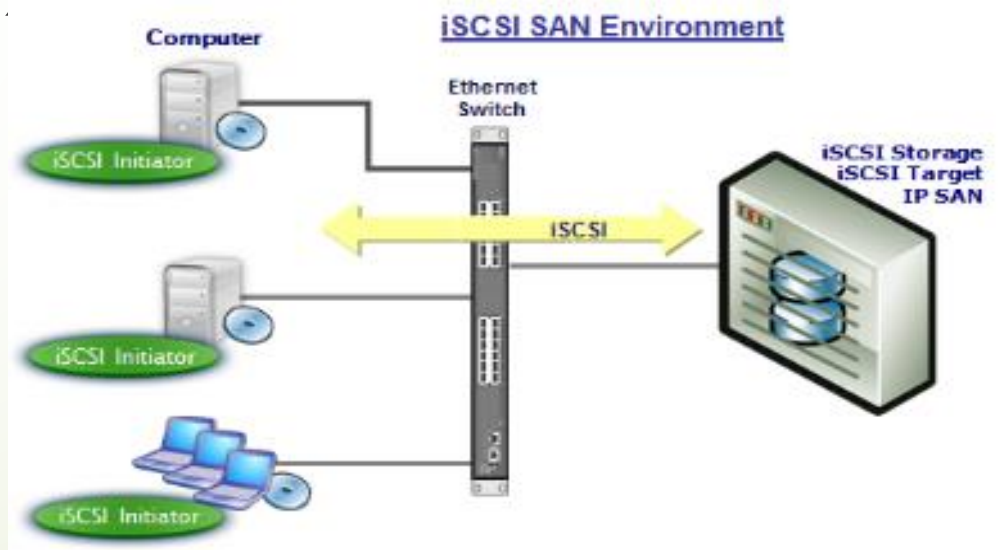
Converged Network: Fibre Channel over Ethernet (FCoE)

- **Transport protocol similar to ISCSI**
- **Operates up to 10gb speeds**
- **Rides on top of Ethernet**
- **Nonroutable**



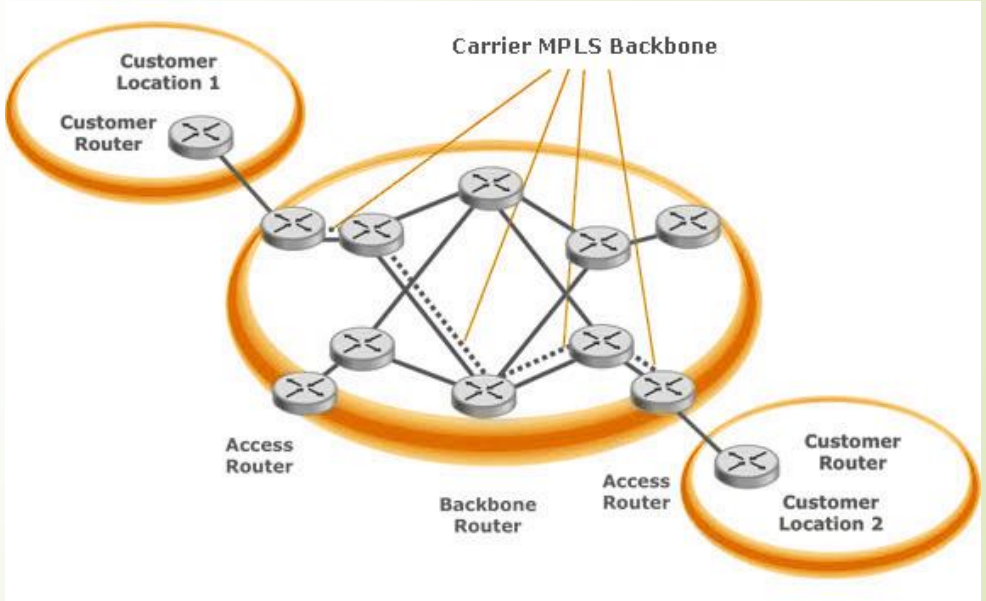
Converged Network: Internet Small Computer System Interface (iSCSI)

- iSCSI is a SAN standard used for connection
  - Replacement for fibre channel
  - Routable (rides on top of TCP/UDP)
  - SCSI signals transmitted over IP



Converged Network: Multi-Protocol Label Switching (MPLS)

- Supports circuit and packet switching
- Forwards frames based on “label” contents
- Allows for variable length frames
- More efficient than ATM (less overhead)



Converged Network: MPLS

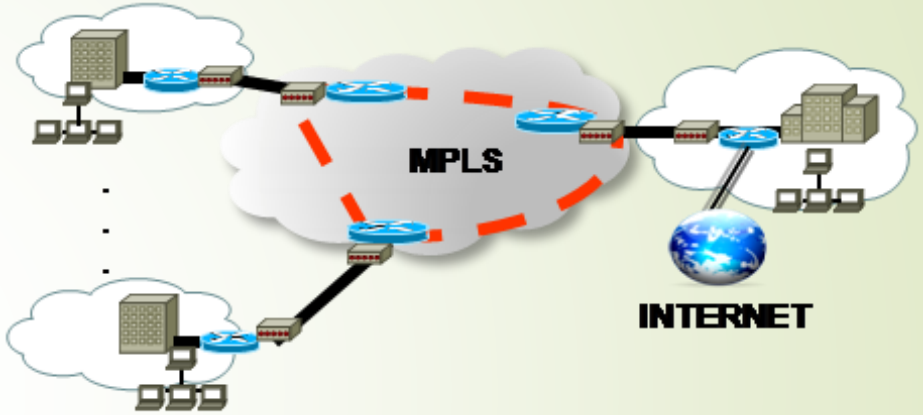
- Couples determinism, speed, and QoS controls of switched technologies (ATM/Frame Relay) with the flexible and robust IP world
- AKA: IP VPN
  - Logically impossible to mix data unless routing device is compromised
  - Provides no encryption services
- For MPLS service level agreements, ensure:
  - Site availability
  - End to end network availability
  - Provisioning time frames

Converged Network: MPLS

- MPLS Label Switched Path ("LSP")
  - One of the most important concepts for the actual use of MPLS
  - Essentially a unidirectional tunnel between a pair of routers, routed across an MPLS network
- An LSP is required for any MPLS forwarding to occur
- MPLS Router Roles/Positions
  - Label Edge Router ("LER") or "ingress node"
    - The router which first encapsulates a packet inside an MPLS LSP
    - Also the router which makes the initial path selection
  - Label Switching Router ("LSR") or "transit node"
  - A router which only does MPLS switching in the middle of an LSP
  - Egress Node
    - The final router at the end of an LSP, which removes the label

Converged Network: MPLS

- MPLS router roles
  - P-provider router
  - PE-provider edge router
  - CE-customer edge



- An LSP is a network wide tunnel but a label is only a link-local value. LSP's are mapped to label values

- Two main routing protocols
  - Label Distribution Protocol (LDP)
  - Resource Reservation Protocol with Traffic Engineering (RSVP-TE)

Converged Protocols - Voice-over-IP (VoIP)

- Combines voice and data over same IP network
- Session Initiation Protocol (SIP)
  - TLS, MD5, Caller ID Suppression
  - Uses call managers and voice gateway systems to setup and teardown voice sessions
- Skype (PC to PC “free”, PC to Landline=$)
- Supports E911
- Uses RTP to maintain real-time communications
- H.323 (ITU standard)
  - Similar to the ISDN call model
  - Serves as an intermediary protocol for migration to pure VoIP solutions

VoIP Concerns

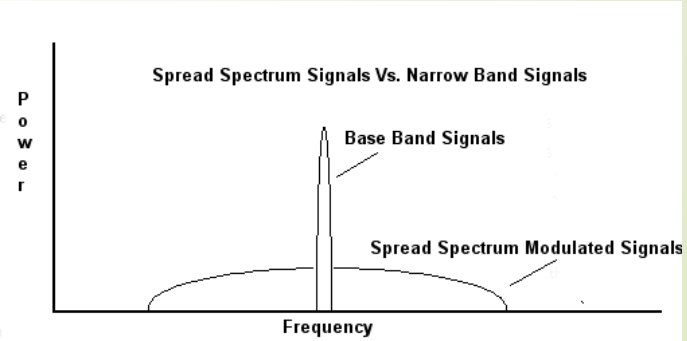
- Packet Loss
- Jitter
- Sequence Errors
- Codec Quality

VOIP Security Issues

- Interception of calls
- Denial of Service Attacks
- Theft of Service
- Exfiltration of data via media session
- Malware embedded in signaling and media session

Converged Protocols - Wireless

- Benefits
  - Convenience, mobility, productivity, easy setup, expandable, and cost
- Wireless Technologies
  - Narrowband
    - Signals transmitted over one frequency (radio station)
  - Spread Spectrum
    - Data spread over multiple frequencies at same time
- Wi-Fi Spectrum 2.4GHz and 5GHz



Wireless – Wi-Fi Variants

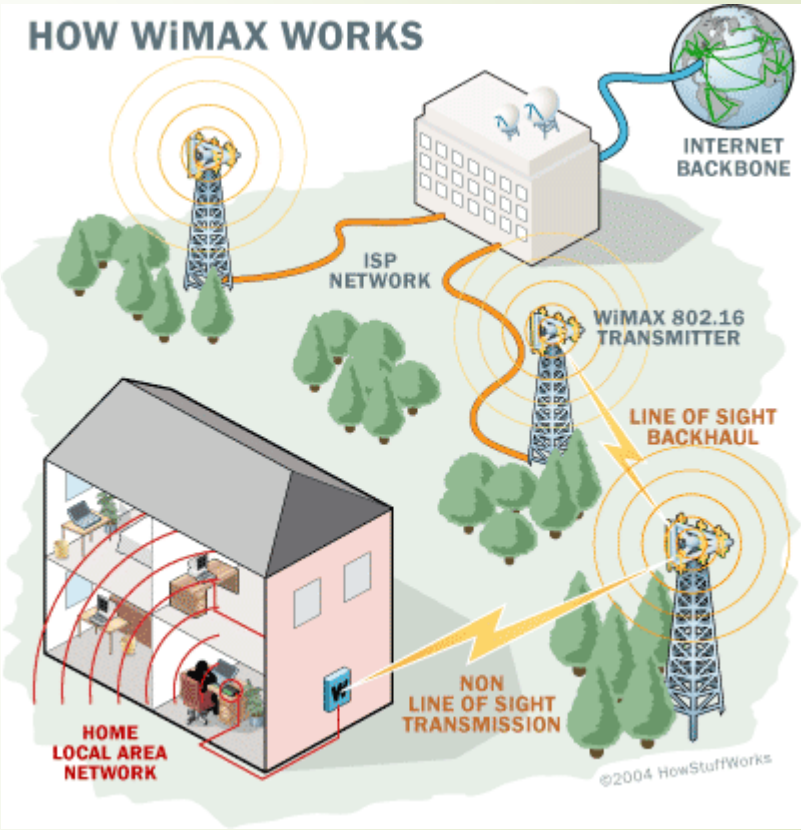
Protocol	Frequency	Modulation	Data Rate
802.11	2.4 GHz	FHSS/DSSS	1-2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	DSSS FHSS legacy	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11n	2.4 / 5 GHz	OFDM	600 Mbps (300 actual)

Wireless - BlueTooth

- Bluetooth (802.15.1) (ZigBee 802.15.4)
- Uses 2.4 GHZ range (bounces between 75 channels)
- Version 2.1 and earlier are limited to 3mbs
- Three classes:
  - Class 1: 100 meters
  - Class 2: 10 meters
  - Class 3: under 10 meters
- Bluetooth Hacking
  - Bruteforce Pairing
  - Bluebugging
  - Bluejacking
  - Bluesnarfing
  - Bluetooth Sniper Rifle

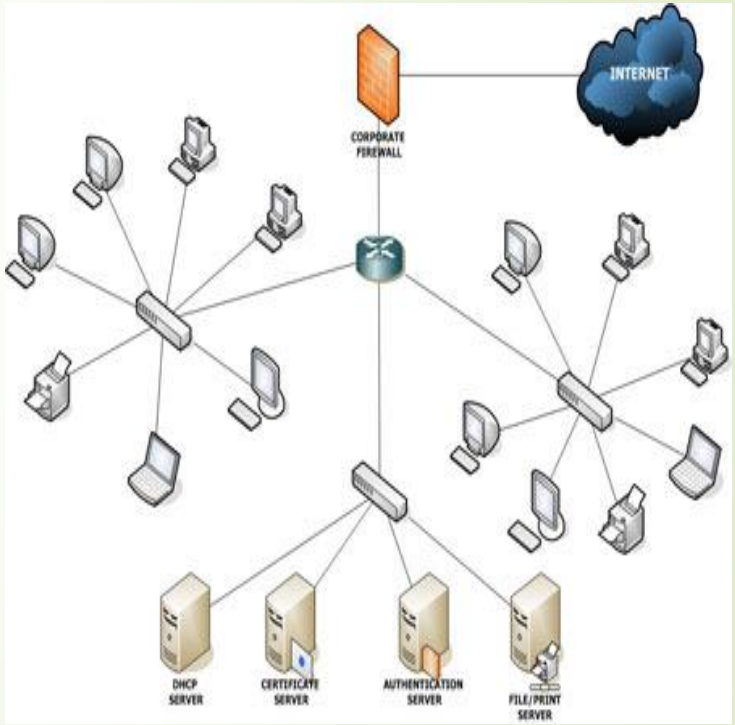
Wireless - WiMAX

- Broadband Wireless
- Up to 30 megabits/sec
  - Varies with distance from transmitter
- WiMAX
  - 802.16 Standard
  - Common alternative for “last mile” broadband access



Types of Networks

- LAN (Local Area Network)
- WAN (Wide Area Network)
- MAN (Metropolitan Area Network)
- GAN (Global Area Network)
- PAN (Personal Area Network)

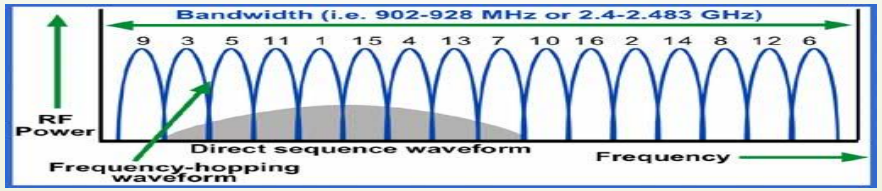


Wireless - Mobile Cellular Telephony

- Code Division Multiple Access (CDMA)
  - Gives a unique code to each call and spreads it over the available frequencies
- Global System for Mobile Communications (GSM)
  - Frequency is divided into timeslots for individual phones to use
- Long Term Evolution (LTE)
  - Uses frequency and time division multiplexing. Upgrade for CDMA/GSM carriers

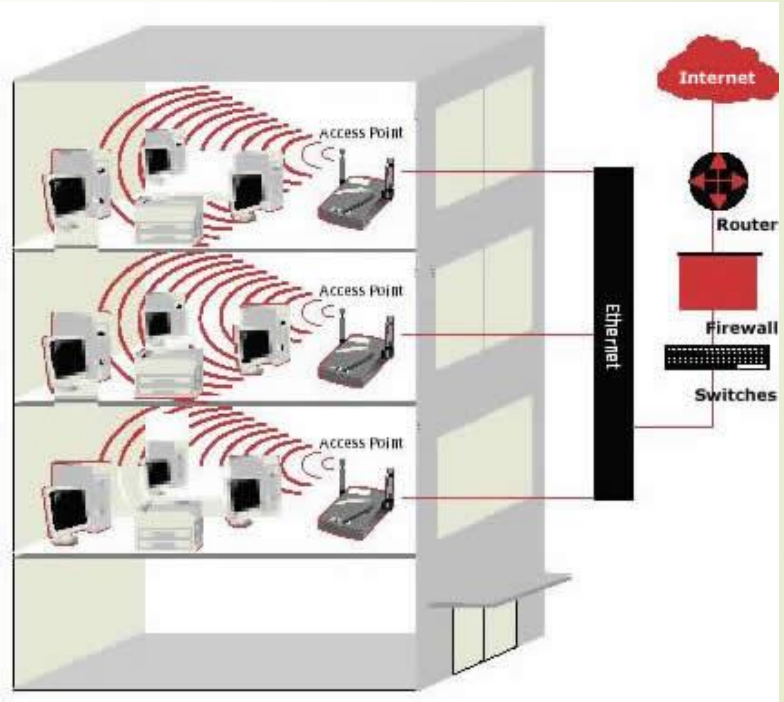
Wireless - Transmission Technologies

- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping Spread Spectrum (FHSS)
- Orthogonal Frequency Division Multiplexing (OFDM)
- Vectored Orthogonal Frequency Division Multiplexing (VOFDM)
- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)



Wireless - Security Issues

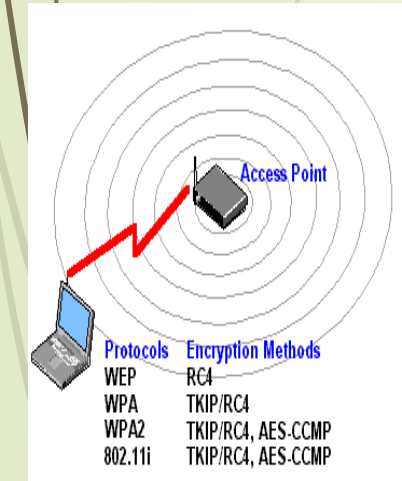
- Authentication
  - Open System Authentication (OSA)
  - Shared-key authentication
  - MAC address tables
  - SSID (broadcast in beacon frame)
  - SSID Naming conventions



Wireless - Wired Equivalent Privacy (WEP)

- Poor/weak crypto design
- 40/104 bit key length
- 24 bit Initialization Vector
- Uses RC4 streaming cipher

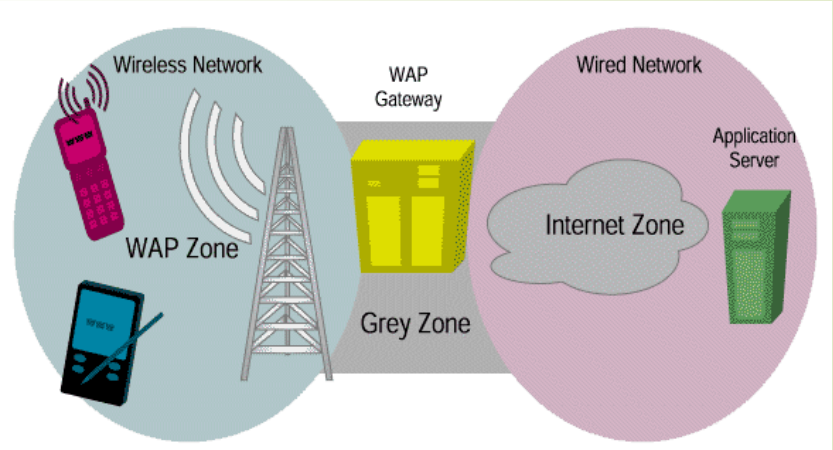
Wireless - Wi-Fi Protected Access (WPA & WPA2)



- WPA (WIFI Protected Access)
  - Improvement to WEP, based on LEAP/TKIP
  - Uses RC4 and Temporal Key Integrity Protocol
  - 48 bit IV128 bit encryption wrapping WEP
- WPA-2
  - 802.11i = security standard
  - Extensible Authentication Protocol (EAP) framework
    - EAP-TLS (Transport Layer Security)
    - EAP - TTLS (Tunneled TLS)
    - EAP-PEAP (Protected EAP)
  - FIPS 140-2 Compliant
  - Supports 128/256-bit AES

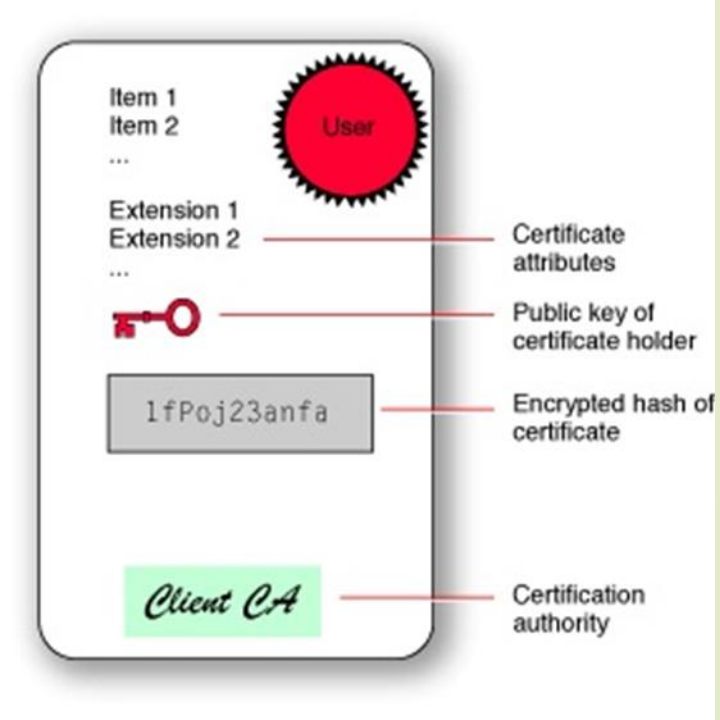
Wireless - Wireless Application Protocol (WAP)

- WAP (prior to version 2)
  - Wireless Application Protocol
  - Includes the WAP Datagram Protocol (UDP emulator)
    - Includes support for WTLS
  - Provides HTTP access from a Mobile/PDA device
  - Mobile devices use Micro-Browsers
  - Created a "WAP Gap"
  - Requires a WAP Gateway system
    - Converts between WML and HTML



Converged Protocols – Public Key Infrastructure (PKI)

- X.509 (PKI)
  - Most widely used standard for defining digital certificates
  - Defines what can go into a certificate, usage, authorities, etc.
  - Not used with PGP/GPG

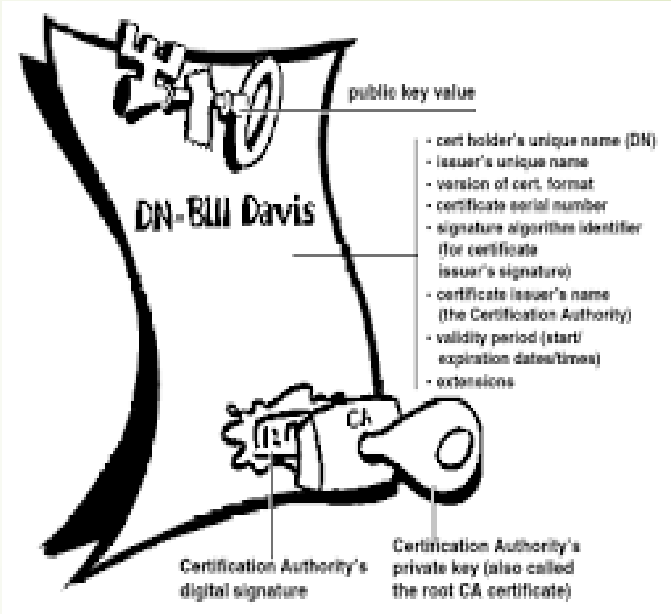


Converged Protocols – X.509v3 Certificates

- Binds a distinguished name to a public key
- Distinguished name abbreviations:
  - Uid –user ID
  - e – email address
  - cn – the user's common name
  - o – organization
  - c – country
- Distinguished name is also used in the Lightweight Directory Access Protocol (LDAP)

X.509v3 - Data Section Contents

- Data Section:
  - Version number
  - Serial number
  - User's public key
  - Public key algorithm
  - DN of CA
  - Valid period
  - DN of certificate subject
  - Optional certificate extensions (client SSL, server SSL, etc.)



- Signature Section
  - Algorithm used in created CA digital signature
  - CA's digital signature

X.509v3 - Components

- Certificate Authority (CA)
  - Creates certificates to authorized users
- Registration Authority (RA)
  - Used to offload the work of the CAs
  - Validates subscriber's identity
  - Distributes keys
- Certificate Server
  - Maintains a database (repository) that stores the certificates

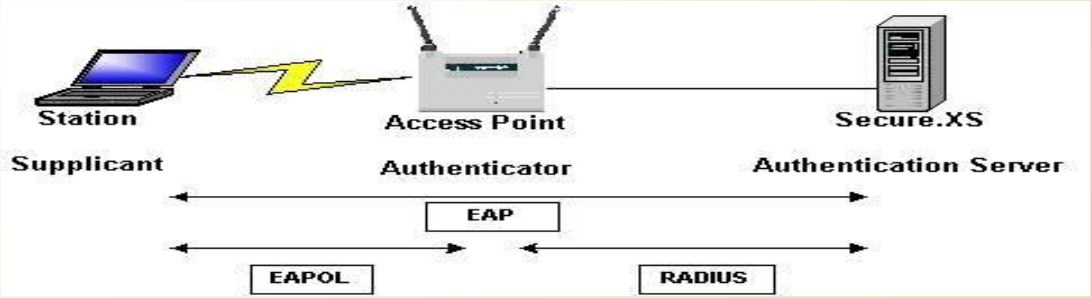
Converged Protocols – Certificates & Authentication

- Password Based Authentication

- Certificate Based Authentication
  - Types of certificates
    - Client SSL Certificate
    - Server SSL Certificate
    - S/MIME Certificate
    - Object Signing Certificate
    - Certificate Authority Certificate

Certificates & Authentication - 802.1x

- Port Based Network Access Control (PBNAC)
- Includes the Extensible Authentication Protocol (EAP) framework
- Terms:
  - Supplicant – 802.1x client
  - Authentication Server – server that authenticates the client (RADIUS)
  - Authenticator – device such as a switch or access point (RADIUS client)



Certificates & Authentication - Extensible Authentication Protocol (EAP)

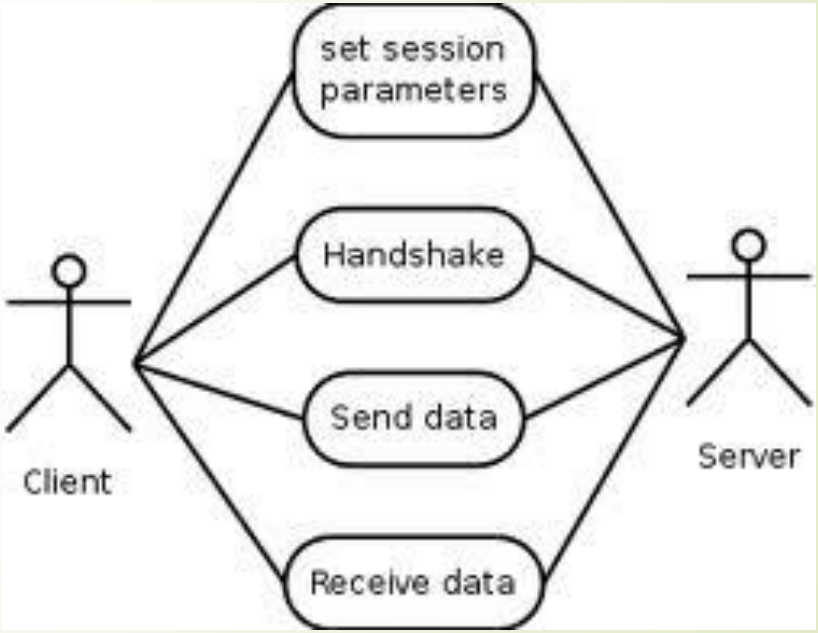
- Many types of EAP (methods)
- Examples:
  - EAP-MD5 (weak, no mutual authentication, crackable)
  - LEAP (Cisco Proprietary, significant flaws, don't use)
  - EAP-FAST (Flexible authentication via secure tunneling) designed to replace LEAP)
  - EAP-TLS (mutual authentication, PKI, TLS)
  - EAP-TTLS (easier to deploy than TLS, No client-side certificate)
  - PEAP (protected EAP, similar to EAP-TTLS, Cisco proprietary)

Certificates & Authentication - Secure Socket Layer (SSL)

- TCP port 443
- Allows for mutual authentication in version 3
- SSL/TLS
  - Normally accepted that SSL/TLS operate between layer 4 and layer 7
  - The SSL/TLS handshake and session creation would happen at layer 5 while the encryption/decryption would happen at layer 6
  - When the layer 7 application stops sending data, the layer 4 connection closes

Certificates & Authentication - Transport Layer Security (TLS)

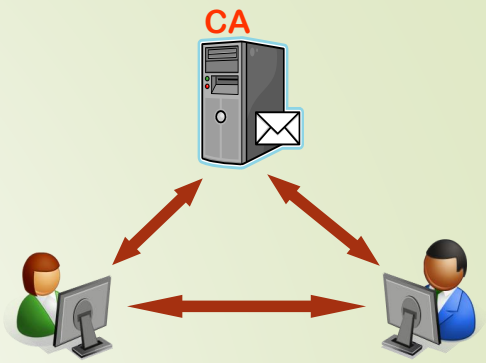
- Successor of Secure Socket Layer (based on SSL v3.0)
- Provides Mutual authentication
- TCP port 443
- Two protocols
  - The TLS Handshake Protocol
  - The TLS Record Protocol



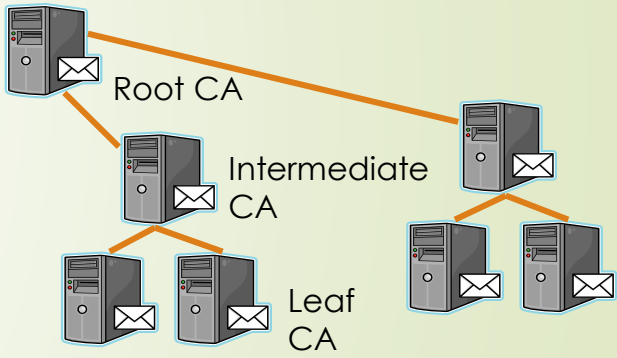
Certificates & Authentication - Secure/Multipurpose Internet Mail Extension (S/MIME)

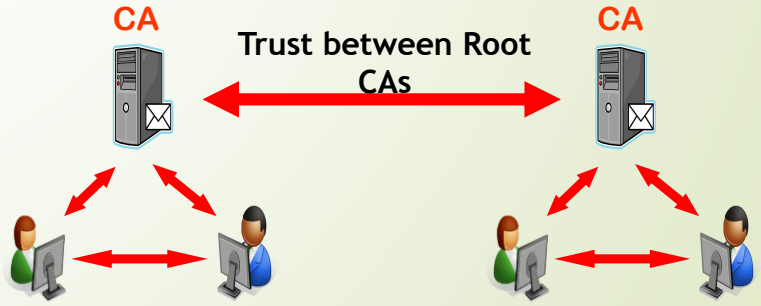
- Standard for public key encryption and signing of e-mail encapsulated in MIME
  - Provides confidentiality, authentication, integrity, and non-repudiation
  - DSS or SHA1 for digital signatures
  - 3DES for encryption of the message
  - Diffie-Hellman or RSA for encryption of the session key
  - Requires PKI (x.509)
  - Hierarchical trust
- Older Protocols
  - MIME Object Security Services (MOSS)
  - Privacy Enhanced Mail (PEM)

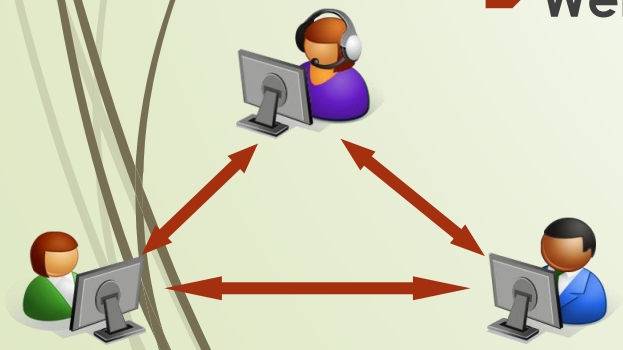
Certificates - Trust Models



- Establish a trust model when dealing with PKI environments
- Four different types:
  - Single Authority Trust (also known as the third-party trust)
  - Hierarchical Trust
  - Hybrid Cross Certification
  - Web of Trust (aka the Mesh Model)





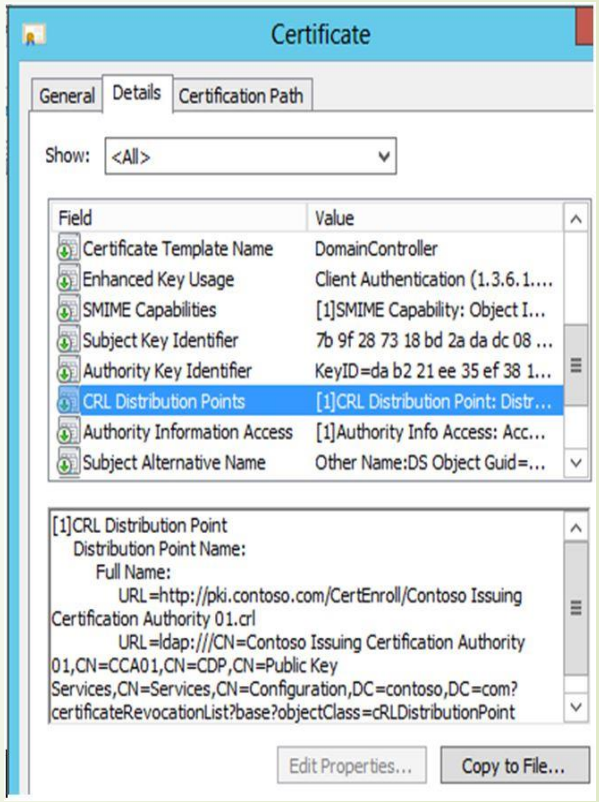


Certificates - Policy & Certificate Practice Statement

- Certificate Policy:
  - Set of rules dictating the circumstances under which a certificate can be used
  - Certificate policy used to protect CAs from claims of loss if the certificate is misused
- Certificate Practice Statement
  - Published document describing:
    - How the CA is structured
    - Which standards and protocols are used
    - How certificates are managed

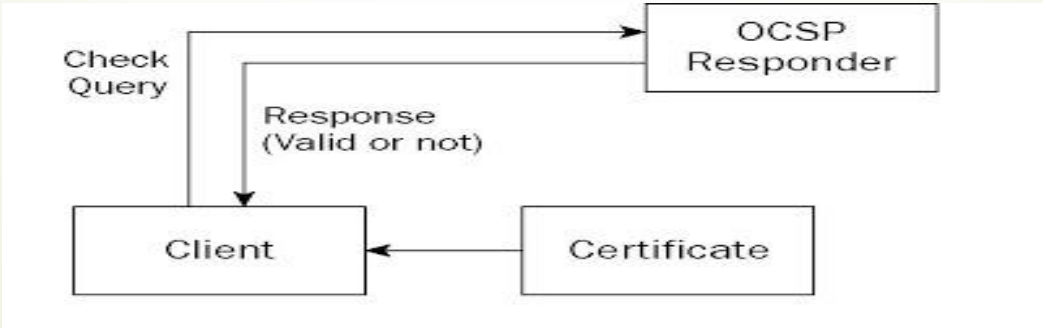
Certificates - Certificate Revocation List (CRL)

- Identifies certificates that have been revoked due to fraud, theft, change in name or relationship with the CA
- Expired certificates are not on the CRL
- Maintained and updated periodically
  - Does not provide up-to-the-moment status
  - Many browsers fail to check CRL
  - Browser uses OCSP for updates



Certificates - Online Certificate Status Protocol (OCSP)

- Used to query the CA as to the status of a certificate issued by that CA
- Particularly useful in large, complex environments
- Responds to a query with a status of valid, suspended, or revoked



Certificate Check Done by Client Querying Responder

Certificates – Suspensions & Renewals

- Suspensions
  - Certificates can be suspended (put on hold)
  - Suspend rather than expire certificates to make them temporarily invalid
- Renewals
  - Unexpired certificates can be renewed close to the end of the expiring certificate's lifetime
  - Allows the same certificate to be used past the original expiration time
  - Bad practice (key life extended)

Certificates - Destruction

- Establish policies for destroying old keys
- When certificate is no longer useful, destroy and remove from the system
- When destroyed, notify the CA so the CRL and OCSP servers can be updated

Converged Protocols – Pretty Good Privacy (PGP)

- **Hybrid Cryptographic System**
- **Performs data encryption, digital signatures, and key distribution**
- **Provides confidentiality, authentication, integrity, compression**
- **Weakness: peer-to-peer trust (not x.509)**

Securing Network Components

- Secure Routing / deterministic routing
  - WAN connectivity is supplied based upon a limited number of different routes
- Boundary routers
- Security perimeter
  - The perimeter of your network — the part that touches the outside world — is where you can make some of the biggest gains in network security

Securing Network Components con't

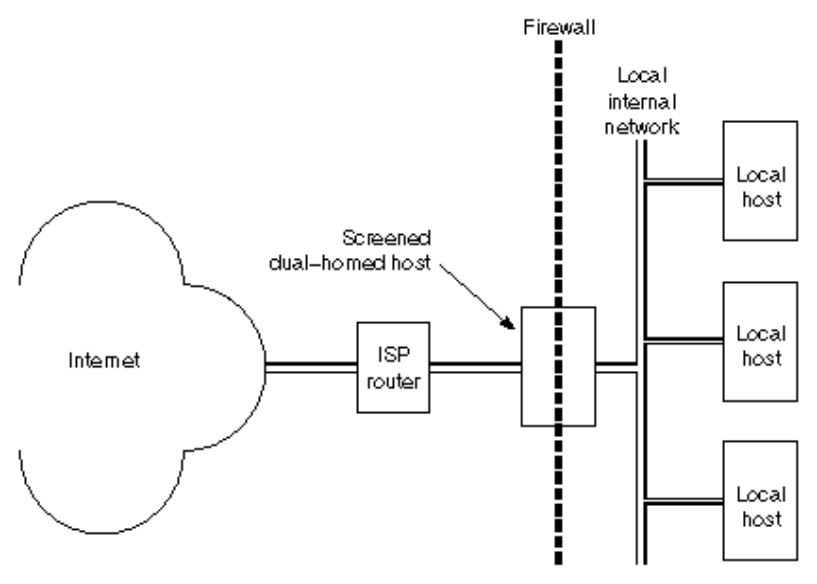
- Non-Blind Spoofing
  - Attack comes from the same subnet
  - Sequence and acknowledgement numbers sniffed
  - Corrupting data stream of established connection
  - Reestablishing connection using correct sequence and acknowledgement numbers (attacker)

- Blind Spoofing
  - External attack
  - Send packets to target to sample sequence numbers
  - Sequence numbers have to be predicted by the attacker

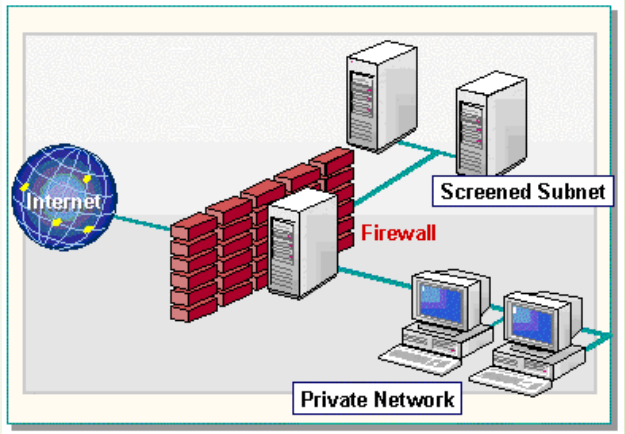
- Man in the Middle Attack (MITM)
  - Both spoofing attacks are examples of MITM attacks

Securing Network Components con't

- Security Perimeter
  - 1st line of protection between the trusted and untrusted networks
  - Usually includes a firewall & router

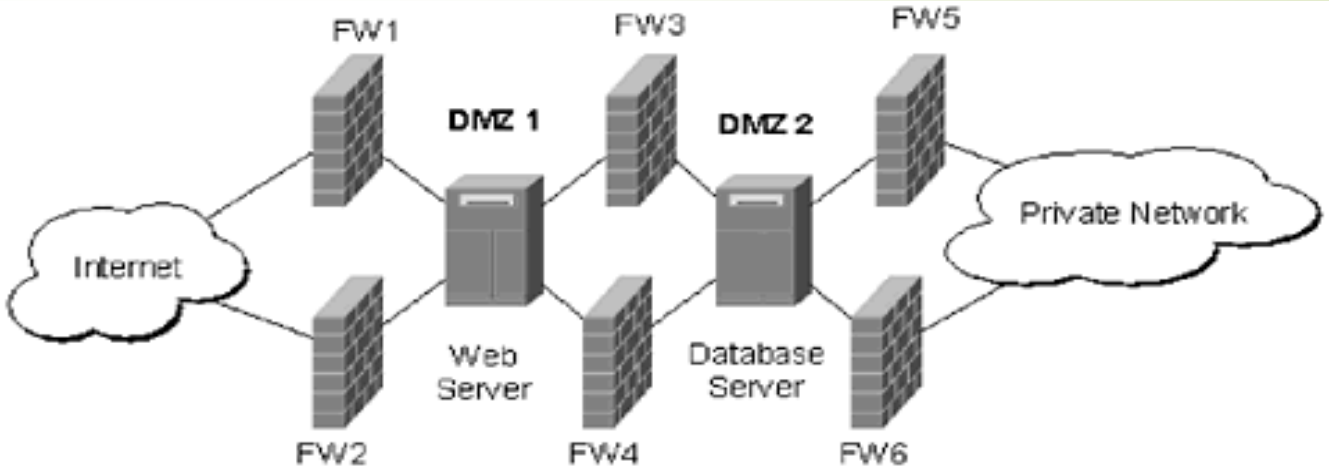


- Network partitioning
  - Dual-homed (multi-homed)
    - Two interfaces (one private, other public)
  - Bastion host
    - Locked down to provide maximum security
    - Bastion hosts commonly reside in DMZ
      - Exposed to untrusted parties



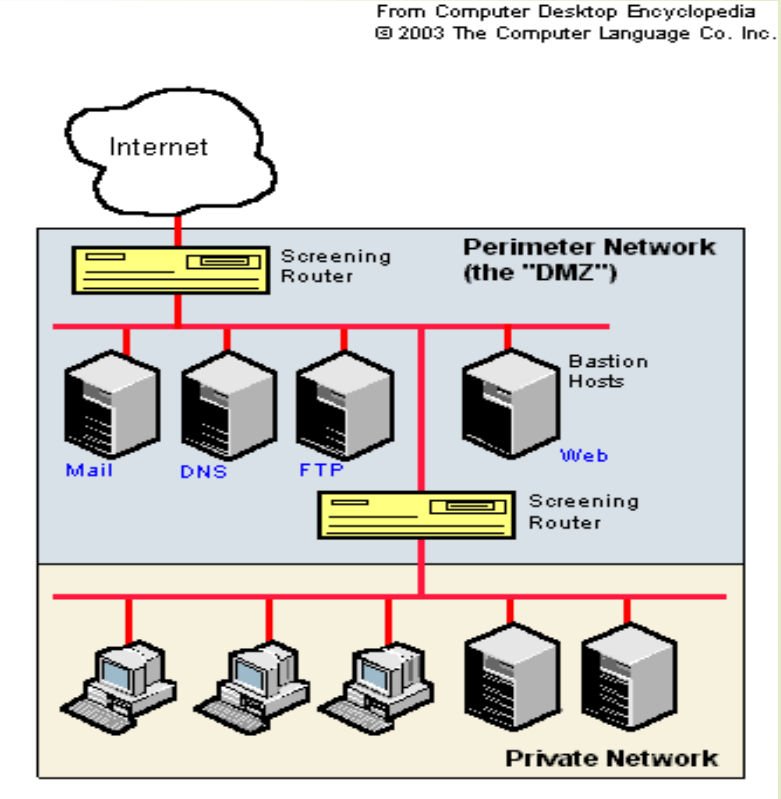
Securing Network Components con't

- **Firewall Architectures**
  - **Single-tier**
  - **Two-tier**
  - **Three-tier**



Securing Network Components con't

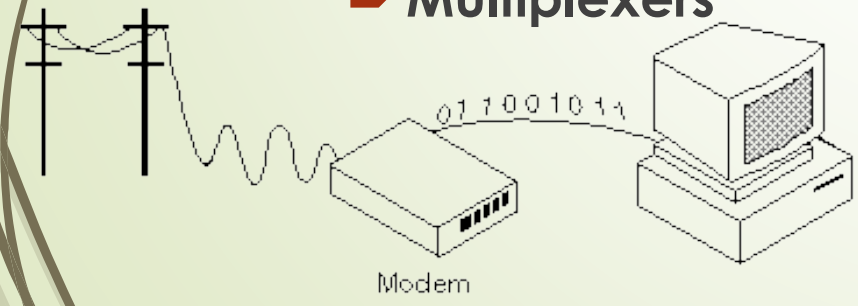
- Demilitarized Zone (DMZ)
  - Neutral Zone, or Screened Subnet
  - Allows us to implement protections and restrictions we feel are necessary

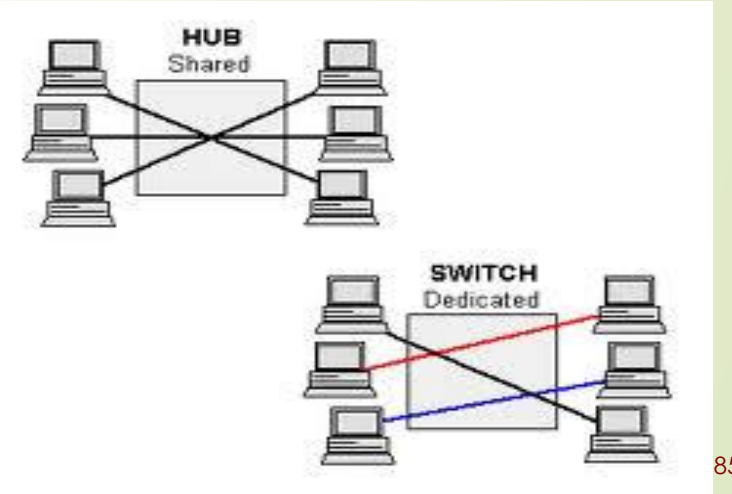


Securing Network Components con't

Securing Network Components con't

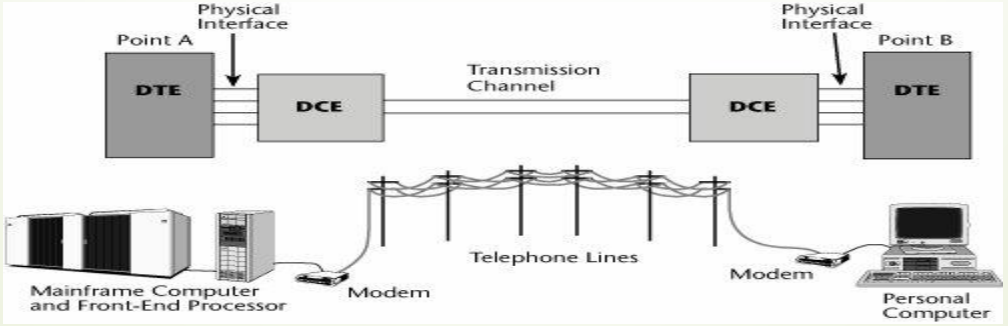
- Hardware
  - Modems
  - Concentrators
  - Front-End Processors
  - Multiplexers
  - Hubs & Repeaters
  - Bridges & Switches
  - Routers



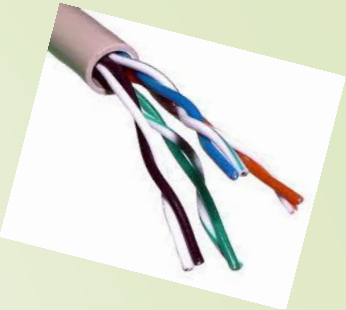


Hardware - DTE/DCE & CSU/DSU

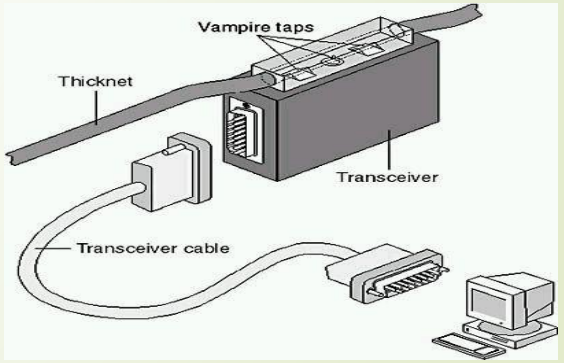
- **DTE (data terminal equipment) desktop, server, etc.**
- **DCE (data communication equipment) router "connects DTE"**
- **CSU/DSU (channel service unit/data service unit) modem "maintains the synchronous timing"**



Cabling



- Transmission Media
  - Cable
    - Twisted pair
    - Coaxial Cable
    - Patch panels
    - Fiber Optics



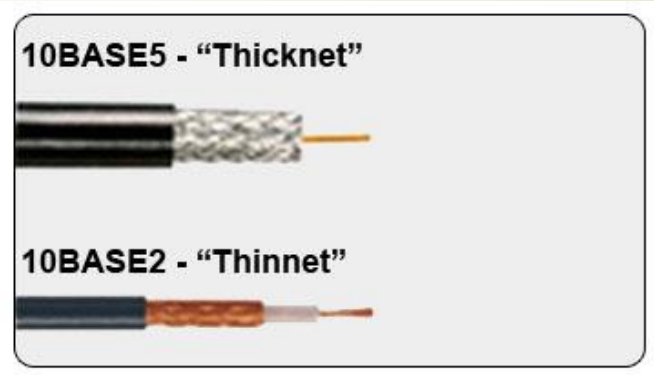
Cable – Twisted Pair

The UTP Categories

Cat 1	Data rate up to 1Mbps - Traditional Telephone & ISDN - Modem
Cat 2	Data rate up to 4 Mbps - Token Ring
Cat 3	Data rate up to 10Mbps - Token Ring & 10BASE-T
Cat 4	Data rate up to 16Mbps - Token Ring
Cat 5	Data rate up to 100Mbps - Ethernet (10Mbps), Fast Ethernet (100Mbps) and Token ring (16Mbps)
Cat 5e	Data rate up to 1000Mbps - Gigabit Ethernet
Cat 6	Data rate up to 1000Mbps - Gigabit Ethernet

The 6 different Unshielded Twisted Pair catagories
Max length depends on network topology and protocol
UTP is mostly used in Star Topologies

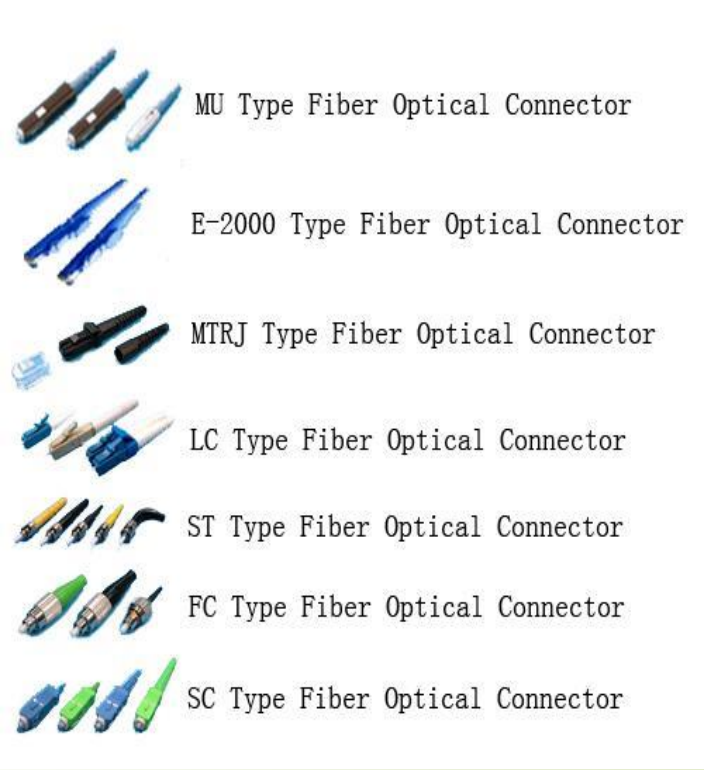
Cable – Coaxial

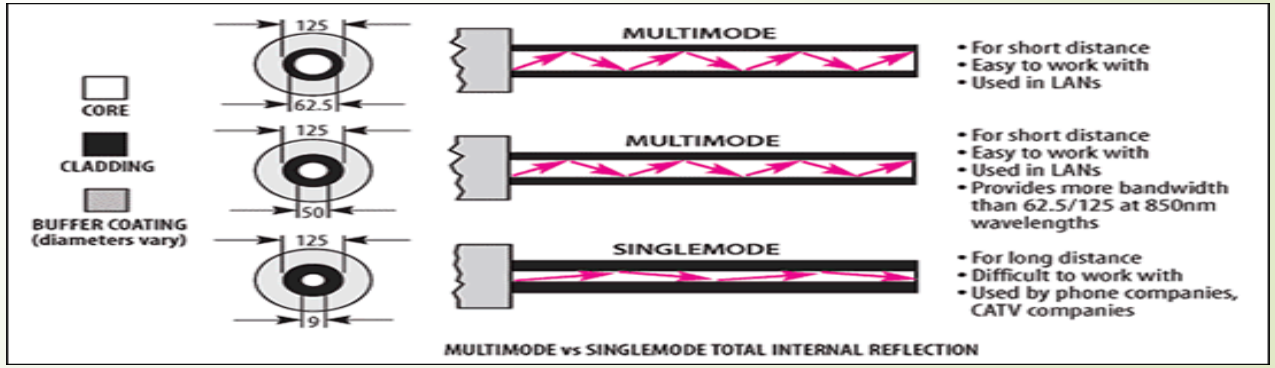


- Coax
  - Thinnet
    - 10Base2 (185 meters)
  - Thicknet
    - 10Base5 (500 meters)
  - Copper conductor surrounded by insulation and a grounded braid
  - Supports longer cable runs
    - Good for broadband

Cable – Fiber Optic

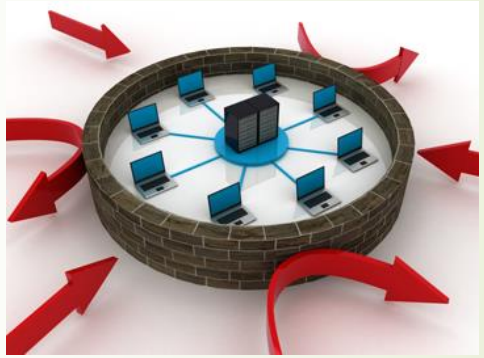
- Fiber (FX)
  - LED, Diode Lasers
  - Immune to EMI and RFI, must physically tap
  - Multiple types of connectors
  - 2 Modes:
    - Multi-mode
    - Single-mode





Securing Network Components - Firewalls

- Hardware
  - Model and capability specific “Turn-key” solutions
  - Pre-defined functions/capabilities
  - Provides maximum performance



- Software
  - May use pre-existing equipment
    - If host operating system not hardened, may leave firewall more vulnerable to attack
  - More expandable (more capabilities)
  - Capable of growth (adding interfaces)
  - TCP Wrappers

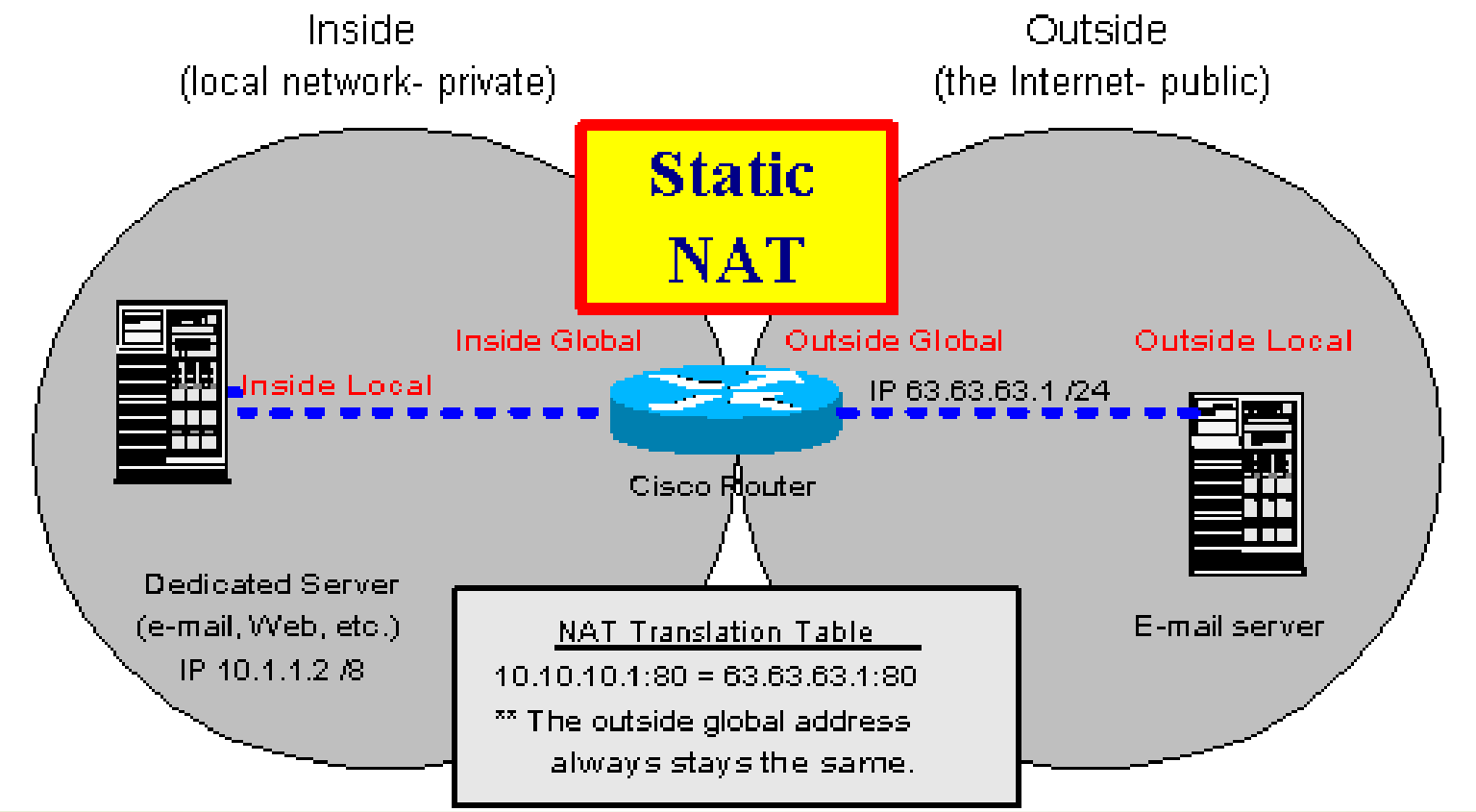
Securing Network Components - Filtering

- Based on a rule set
- Each rule instructs the firewall to block or forward a packet based on one or more conditions.
  - By Address
    - Source address, destination address, or both
  - By Service
    - Determined by destination port or by protocol name

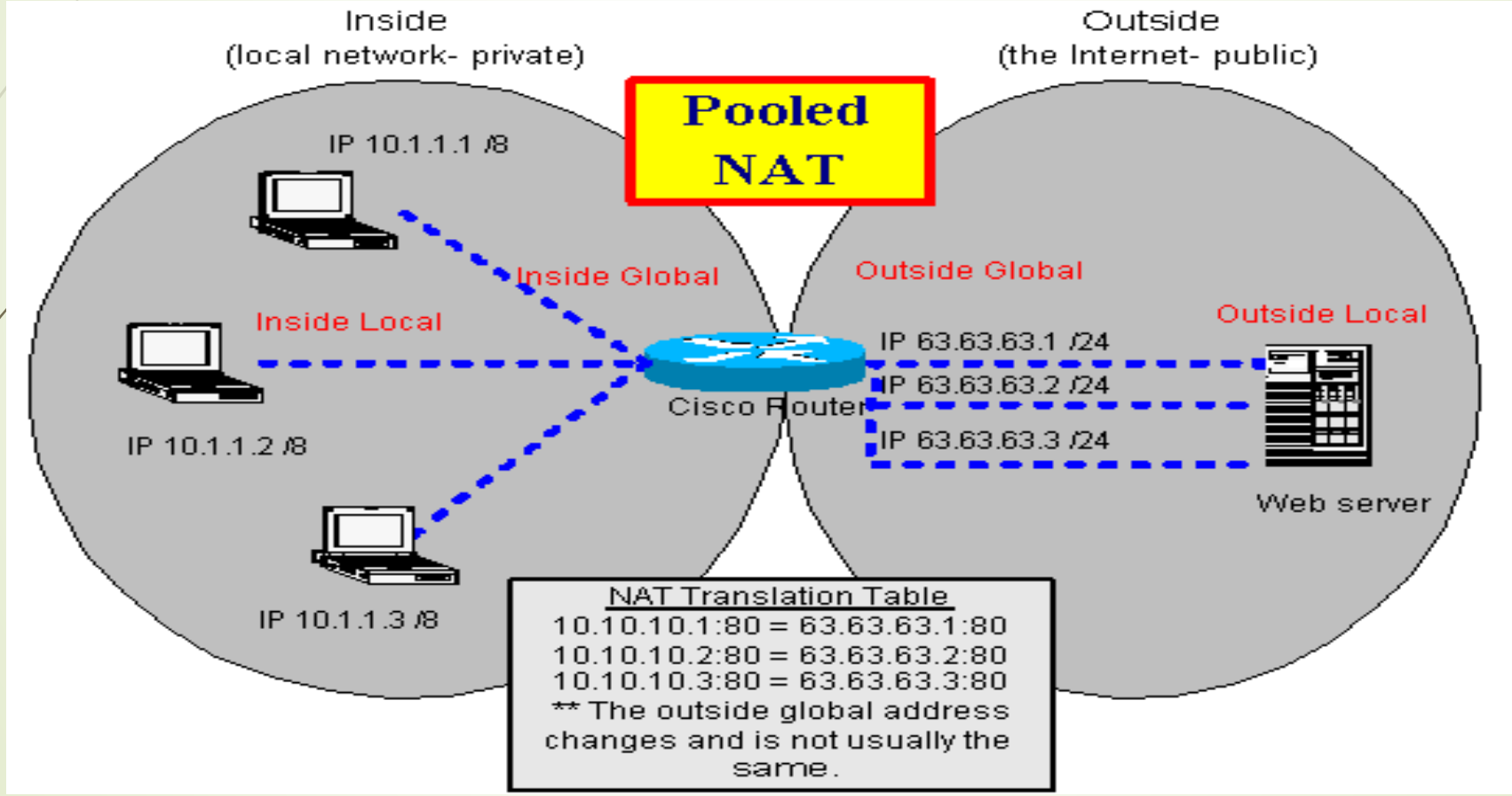
Securing Network Components – Network Address Translation (NAT)

- aka IP Masquerading
  - Conserve IP Address Space
  - Static/Full Cone (one-to-one)
  - Dynamic/Restricted Cone (one-to-many)
    - Port Restricted Cone NAT
    - Symmetric NAT
  - Port Address Translation (PAT (many to one))

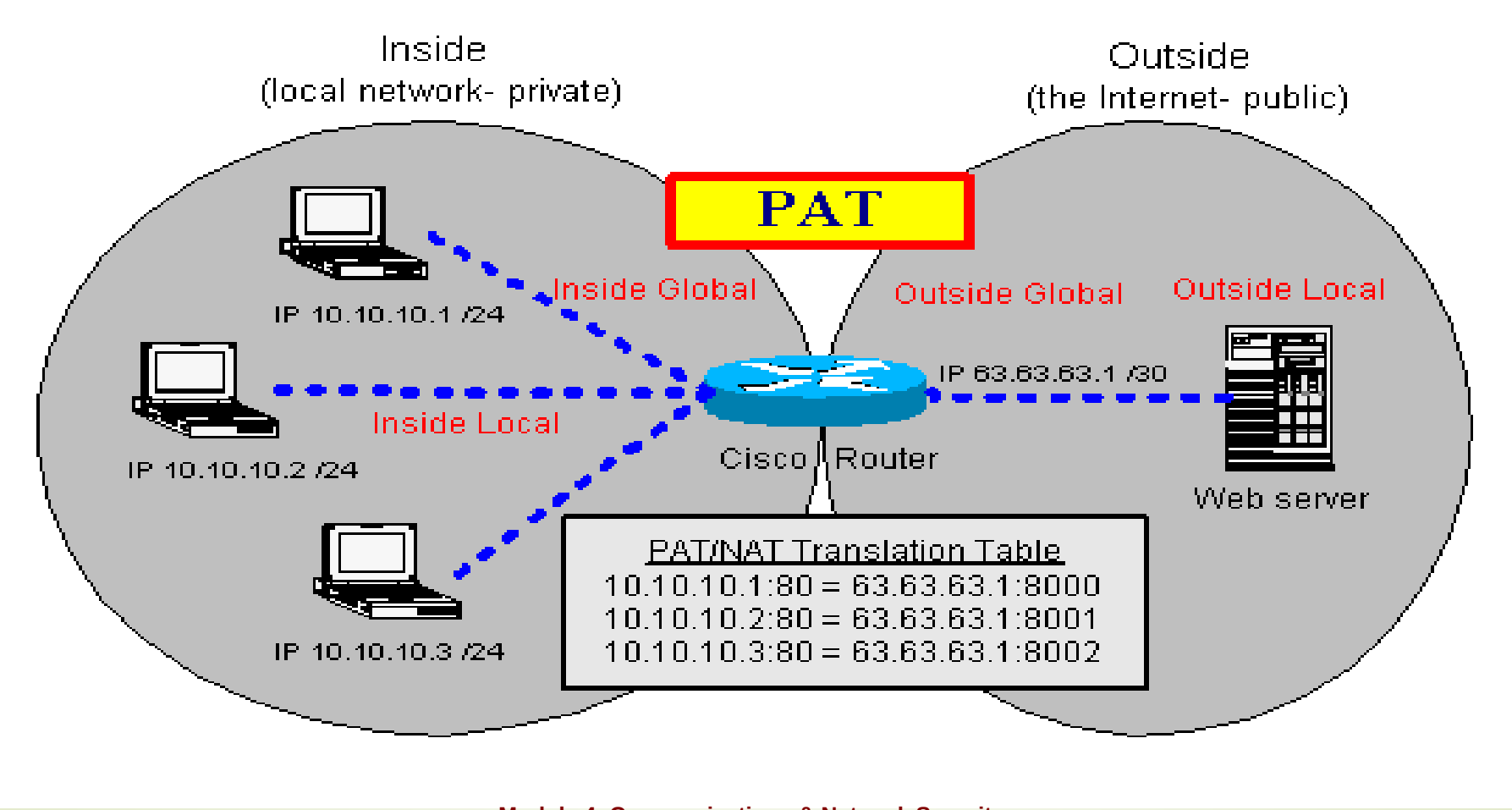
Securing Network Components – NAT (Static)



Securing Network Components – NAT (Dynamic)

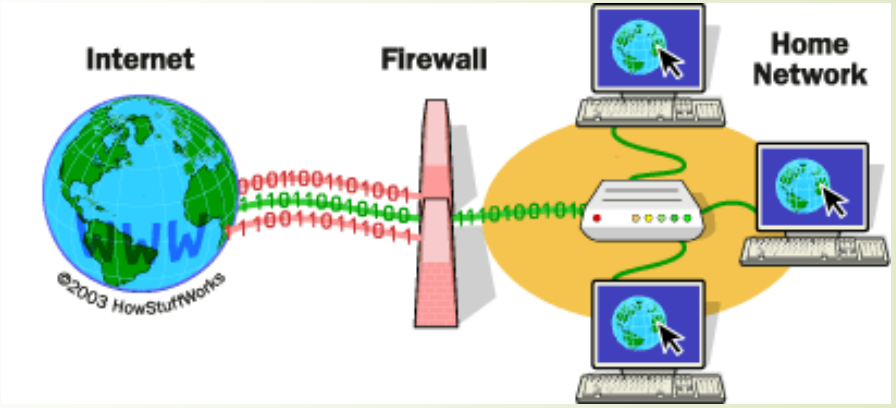


Securing Network Components – Port Address Translation (PAT)



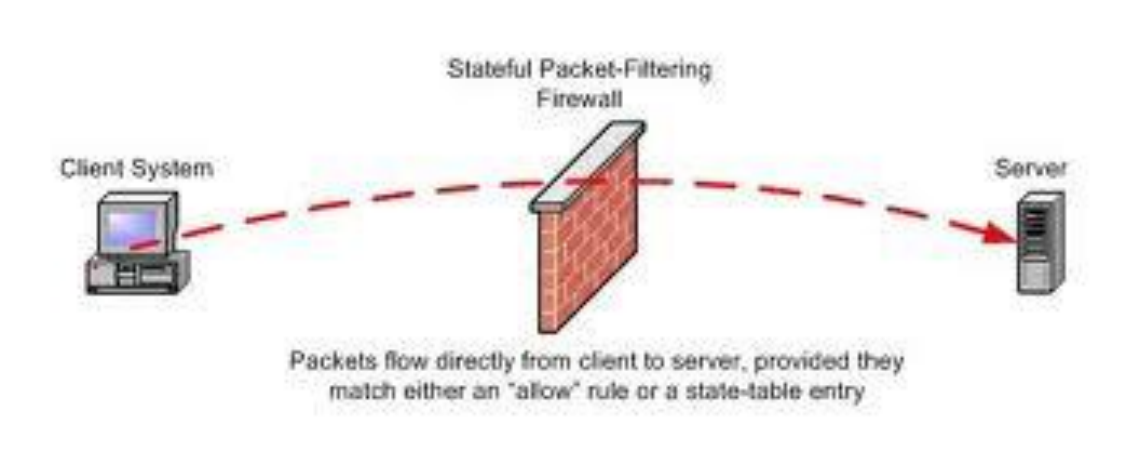
Securing Network Components – Static Packet Filtering

- Examine packet header (packet filtering firewall)
- SRC, SRC PORT
- DST, DST PORT
- PROTO
- First Generation Firewall (high performance)
  - Screening/Common router



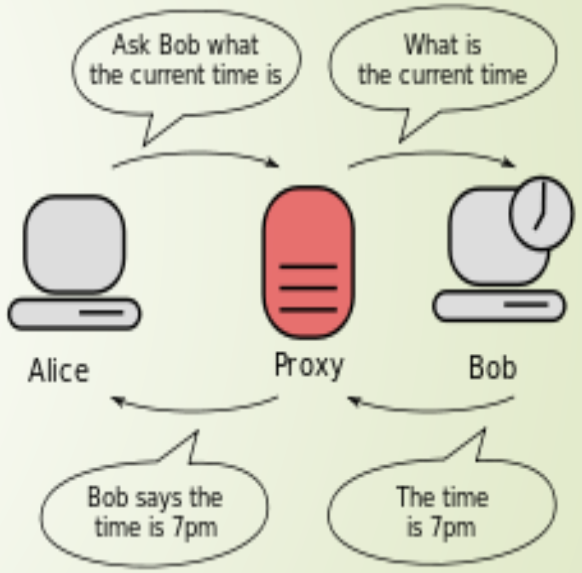
Securing Network Components – Stateful Inspection/Dynamic Packet Filtering

- **Stateful Inspection**
  - **Monitors TCP streams (whole stream, not just handshake)**
  - **Able to dynamically open ports and track sessions for bi-directional protocols (such as FTP)**
  - **Third generation firewall**

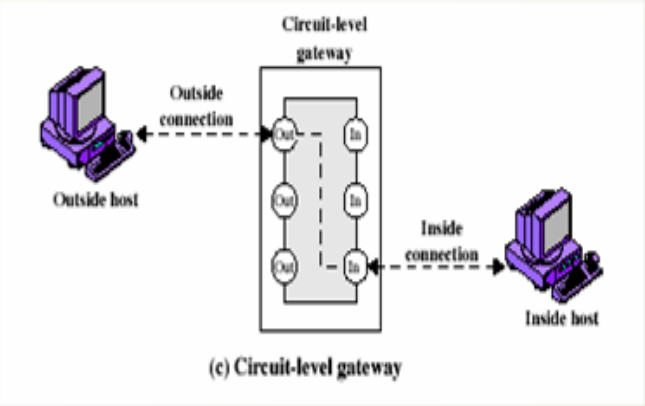


Securing Network Components – Proxies

- Application Level Gateway
  - Proxy firewall, Application protocol aware
    - Ability to hide client information (not just IP address like NAT)
  - Excessive packet examination
    - May cause a reduction in performance
  - Second Generation Firewall (provides isolation by creating virtual circuits with each firewall client)



Securing Network Components – Proxies



- Circuit-Level Gateway Firewalls
  - Raw SOCKS (session layer, secure channel service)
  - Managed based on the circuit
  - Has ability to redirect (port forward) and perform address translation
  - May perform basic TCP or circuit anomaly inspections
  - Also a Second Generation Firewall
  - Not as many access control options as a true Application Proxy Firewall

SOCKS

- SOCKS (SocketSecure)
  - Circuit proxy server with commercial and freeware implementation
  - Layer 5 of OSI model
  - If encryption is supported, can act as a VPN
  - Port 1080

Securing Network Components – End Point Security

- End point security is that added bit of protection you put on the endpoints (PCs)
- Consists of but not limited to:
  - Anti-virus
  - Application white listing
    - Allowing applications to run if they match a known good hash or have a digital signature
  - Removable media controls
  - Disk encryption
  - Honey pots

Securing Network Components – Content Distribution Networks (CDN)

- **Distributed system of servers located in multiple data centers across the Internet**
- **Serves content to users**
- **Goal is high availability and performance**

Secure Communication Channel - FAX Abuse

- Abuse – FAX
  - Not encrypted by default
  - Walk by fax theft
    - Many fax systems are in a common, multi-person access areas
    - Other concerns
      - Human error (entering the wrong number)
  - FAX over internet
    - Use fax encryptor
    - Disable automatic printing
    - Consider using a fax server

Secure Communication Channel - Phone System Abuse

- **Abuse - POTS/PSTN Old school Phreaking (free phone calls)**
  - **Black – box (Home Phone Abuse)**
    - **Voltage manipulator**
  - **Red –box (Pay Phone Abuse)**
    - **Coin tone generator**
  - **Beige/White - box**
    - **Telco Handset, Frequency generator**
      - **DTMF, what phone techs carry**
  - **Blue – box**
    - **Hack the Phone Switch**
      - **Trunk system tone generator**

Secure Communication Channel - Peer-to-Peer (P2P)

- Alter typical client/server model as every system can act as either a client, server or both
  - Centralized (Napster)
  - Decentralized (Gnutella, Bit Torrent)
    - More resilient
    - Little assurance that data received

Secure Communication Channel - Remote Meeting

- Two main implementations
  - Citrix GoToMeeting
  - MicroSoft Office Live Meeting
- Promote sharing of audio and video
- Designed to tunnel via SSL/TLS
- May violate security policy for the sake of connectivity

Secure Communication Channel - Instant messaging

- Extensible Messaging and Presence Protocol (XMPP) and Jabber
- Internet Relay Chat (IRC)
- Proprietary applications and services
- Risks
  - Authenticity
  - Confidentiality
  - Scripting
  - Social engineering
  - SPIM
  - Tunneling Firewalls

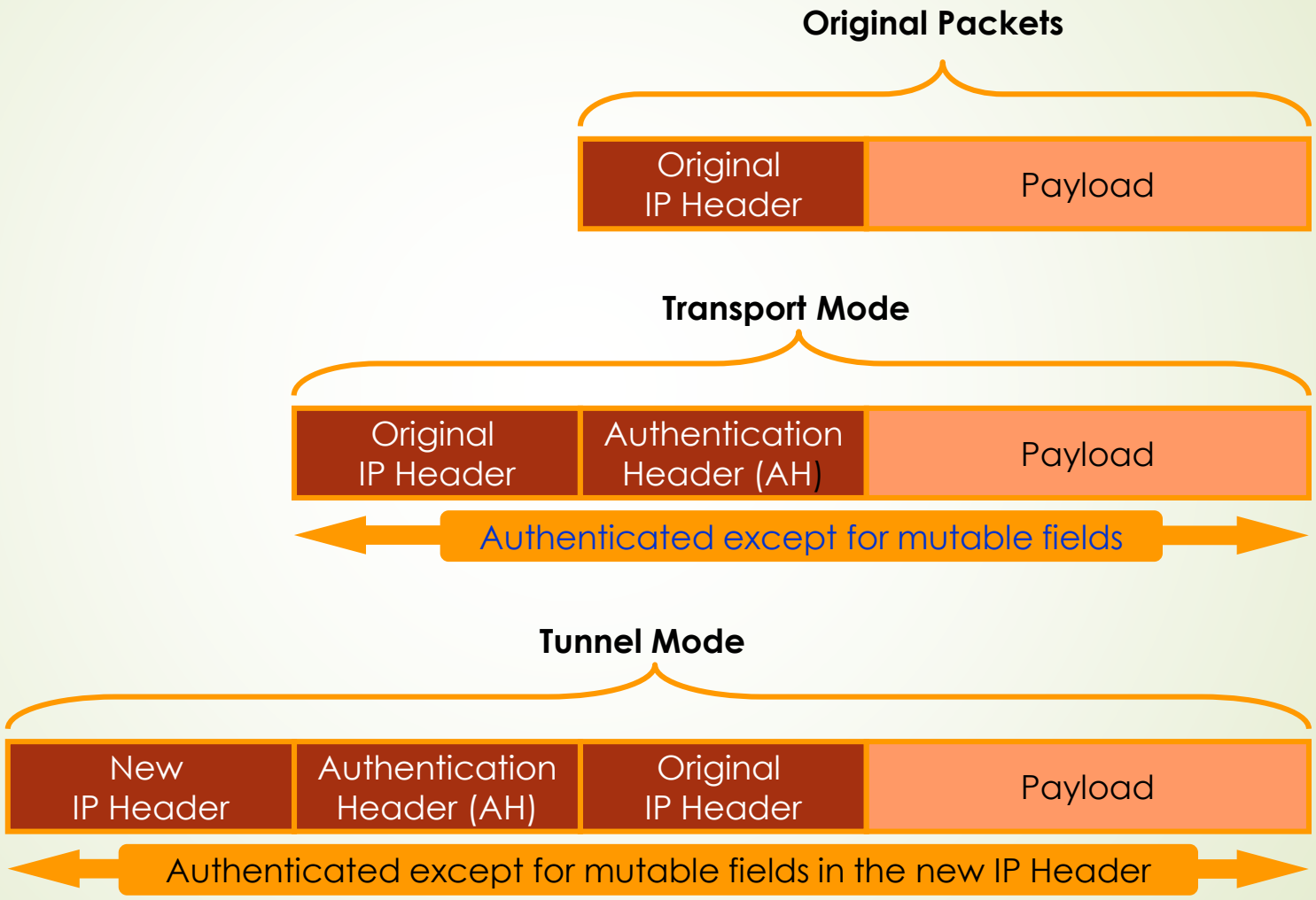
Secure Communication Channels - Internet Protocol Security (IPSec)

- Most widely deployed VPN technology
- Requirement for IP Version 6
- Can be used to encrypt any traffic supported by IP
- Includes both encryption and authentication
- Can be used with L2TP or alone
- Requires either certificates or pre-shared keys
- Operates at Layer 3

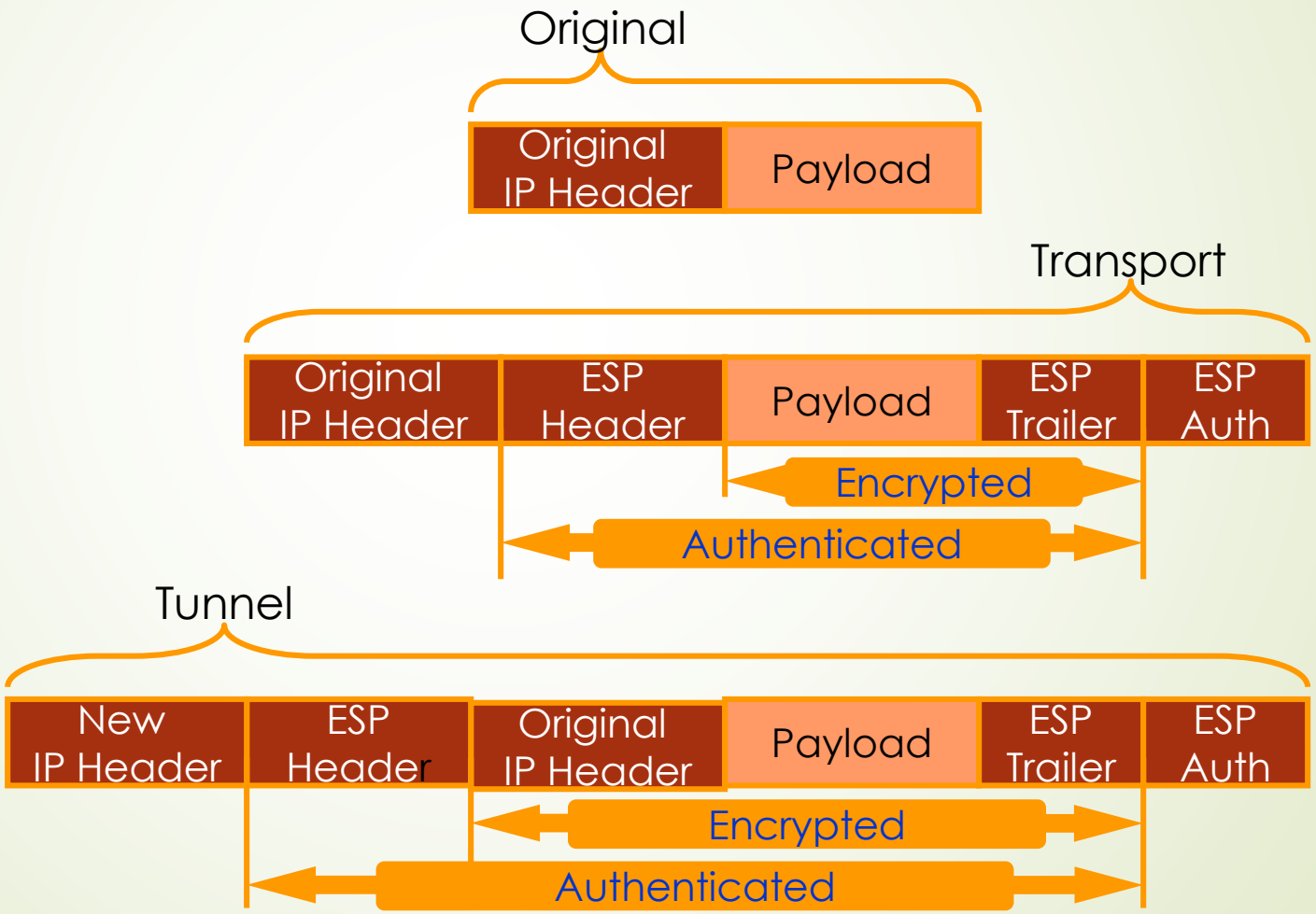
IPSec - Terminology

- Modes
  - Transport Mode
  - Tunnel Mode
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Security Association (SA)
- Security Parameter Index (SPI)
- Internet Key Exchange (IKE)
  - Internet Security Association Key Management Protocol (ISAKMP)
  - Oakley
  - SKEME

IPSec - AH Transport & Tunnel Modes



IPSec - ESP Transport & Tunnel Modes

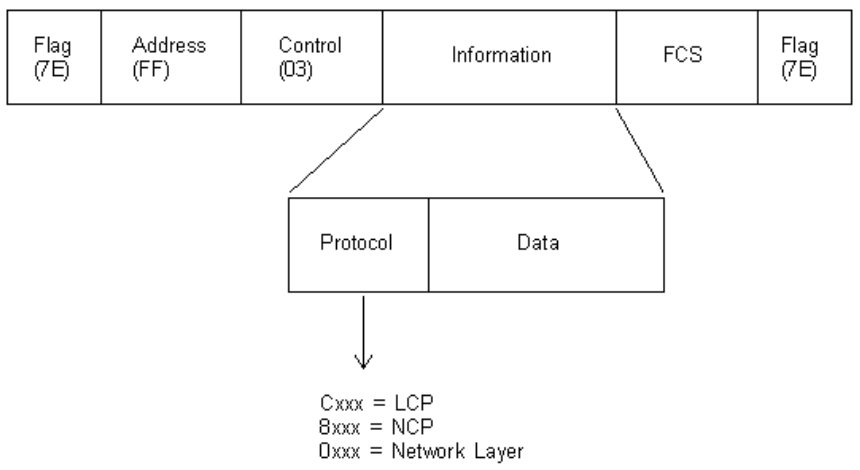


Secure Communication Channels – High Assurance Internet Protocol Encryptor (HAIPE)

- **Extension of IPSec used for highly-secure communications**
- **IP encryption device such as TACLANE, KIV-7, or KG-240**

Secure Communication Channels - Tunneling

- Serial Line Internet Protocol (SLIP)
  - Requires a pre-configured IP Address on each end
  - Only supports TCP/IP, no native error detection



- Point to Point Protocol (PPP)
  - Supports multiple network layer protocols
    - IP, IPX, AppleTalk, NBF
  - PPP over Ethernet
  - PPP over ATM

Secure Communication Channels - Tunneling

- Point-to-Point Tunneling Protocol (PPTP)
  - Encapsulation
  - Encrypts PPP packets
    - Negotiation in the clear
    - After negotiation is completed, channel is encrypted
  - Uses MPPE to encrypt data
  - Uses TCP port 1723

- Layer 2 Tunneling Protocol (L2TP)
  - Hybrid of PPTP and L2F
  - Multiple network protocols supported
  - No data encryption
    - Uses IPSec to provide data encryption and integrity
  - Uses UDP port 1701

Secure Communication Channels

- Centralizes and Extends Authentication Capabilities for Remote Access to Network Resources and Network Access Control
- TACACS+ – Cisco Proprietary
- RADIUS – 802.1x Standard
- DIAMETER – IETF replacement for RADIUS

AAA

- Security capability demanded of remote access servers (Radius, TACACS+, etc.)

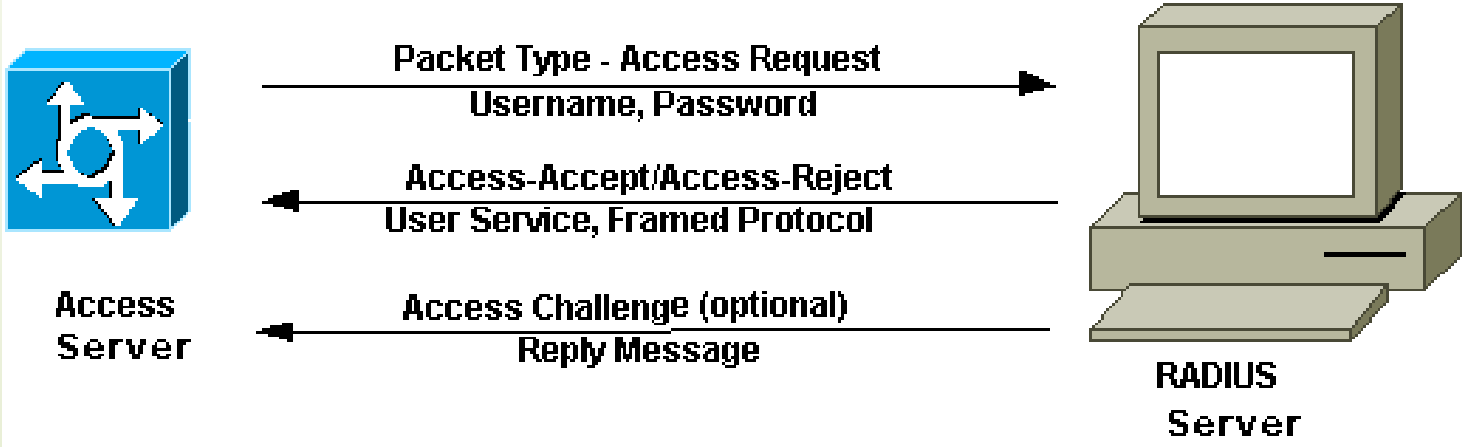
- AAA
  - Authentication
  - Authorization
  - Accounting

Secure Communication Channels – Remote Authentication Dial In User Service (RADIUS)

- Supports AAA but not as separated services
  - Authentication –against a database; specific users access to specific objects
  - Accounting-logs each RADIUS connection
- UDP; port 1812 for transport; 1813 for auditing. RFC 2865
- Supports PAP, CHAP(password may be stored unencrypted),EAP
- Only PW encrypted in transit
- Request and response data carried in Attribute Value Pairs (AVP)
  - RADIUS – 8 bit – 256 possible AVPs

RADIUS CODES

- Access-Request
- Access-Accept
- Access-Reject
- Accounting –Request
- Accounting-Response
- Access-Challenge



Secure Communication Channels – DIAMETER

- Replacement for RADIUS but not fully compatible with RADIUS
- Better performance and encryption
- Single server to handle policies- RADIUS needs more
- It uses TCP port 3868
- Security provided by TLS or IPSEC
- 32 bit – billions of Attribute Value Pairs (AVP) – can support mobile remote users
- Better for roaming support

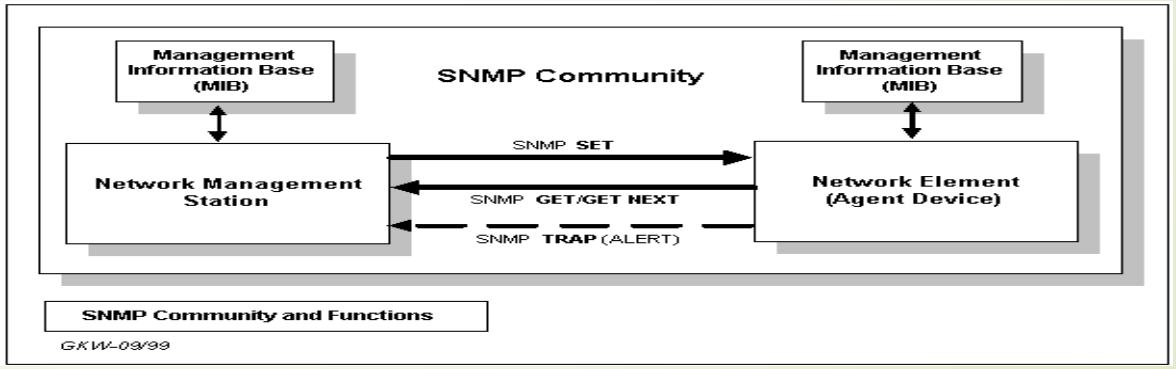
Secure Communication Channels – Terminal Access Controller Access Control System (TACACS+)

- Replaces previous version (TACACS/XTACACS)
- UDP/TCP port 49
- Allows for two factor authentication (static passwords in previous versions)
- Encrypts all data below the TACACS+ header (password and username)
- Similar functionality to RADIUS

RADIUS	TACACS+
UDP: Separate timers	TCP: Automatically adjusts to network conditions
Hashes password only	Encrypts entire message
Authentication/authorization one element	Authentication/authorization distinct elements
Multivendor support	Cisco proprietary
Supports IP	Multiprotocol support

Secure Communication Channels – Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP)
  - Exchange of management information between network devices
  - Version 3 is secure (encryption for passwords)
  - TCP / UDP 161
  - TCP / UDP 162



Secure Communication Channels – Remote Access Services

- TCP/IP Terminal Emulation Protocol (TELNET)
  - TCP 23
  - Username / password authentication in the clear
- Remote Log-in (rlogin), Remote Shell (rsh) Remote Copy (rcp)
  - TCP 513, 514, and 514 respectively
  - Protocols granting remote access to a machine, normally a UNIX server
  - Data transmitted in the clear
    - Solution: SSH for rlogin, rsh and rcp

Secure Communication Channels – Screen Scrapers

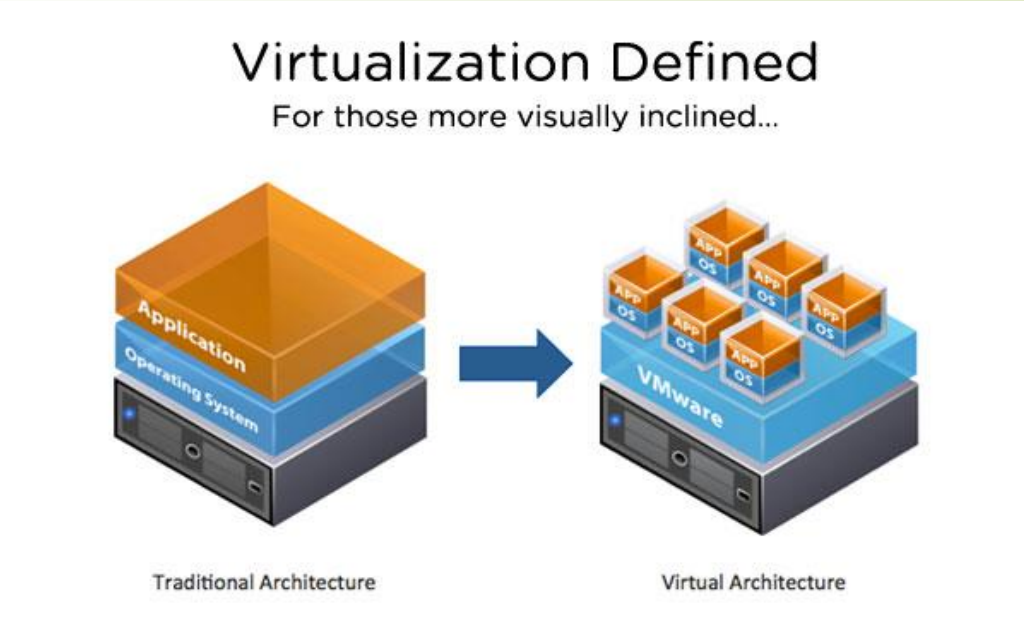
- **Program that extracts data from output on a display**
- **Have legitimate uses when old technology fails to interface properly with modern technology**

Secure Communication Channels – Desktop and Application Virtualization

- VDI (virtual desktop infrastructure or virtual desktop interface)
- Applications can be offered virtually as opposed to a full desktop environment
- Good for legacy applications not compatible otherwise
- Allows for strict access control and quick patching
- Similar to running a thin client or mainframe

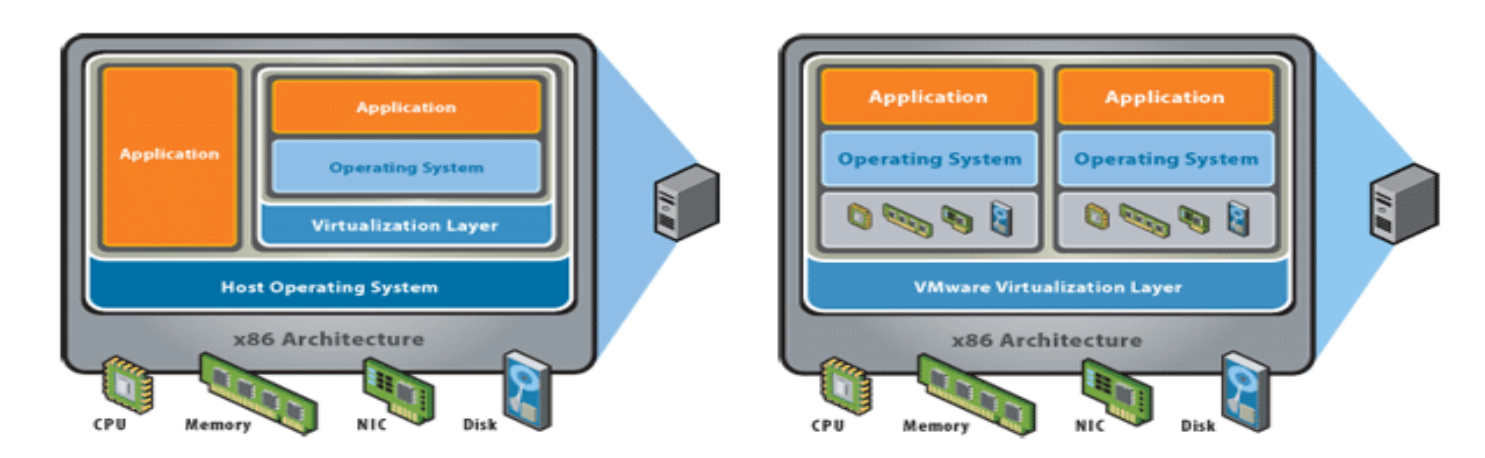
Virtualization

- Not a replacement for a firewall
- Traffic between hosted systems can be invisible to network monitoring software
- Never combine guests with different security needs
- Benefits:
  - Lower overall hardware costs, hardware consolidation, lower power and cooling needs, quicker stand-up of systems, faster backup and recovery, testing, easier patching



Hypervisor

- Controls access between the virtual guest and the physical hardware
- Type 1 (bare metal) hypervisor runs directly on hardware
- Type 2 (Hosted) hypervisor runs as an application



Secure Communication Channels – Remote Desktop

- Tunneling technologies such as IPSec, SSH, or SSL should be used for access

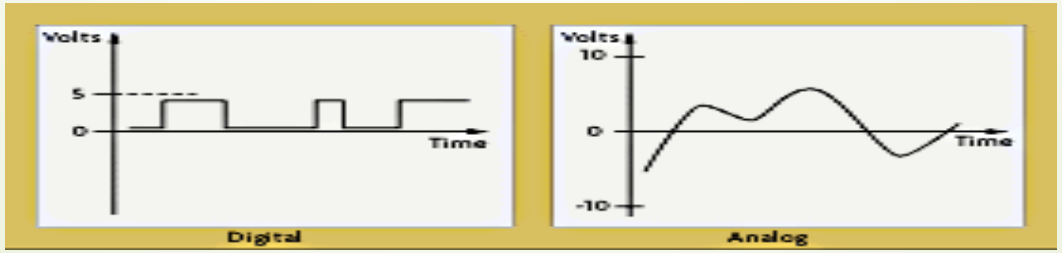
- Examples of access methods:
  - Unix rlogin port 513
  - Unix rsh port 514
  - VNC port 5900
  - Remote Desktop Protocol 3389
  - Reverse Tunnels HTTPS port 443
    - Citrix, GoToMyPC, LogMeIn

Secure Communication Channels – Telecommuting

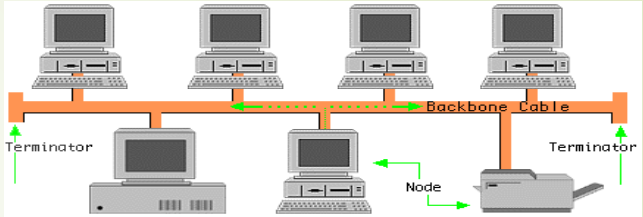
- Is the user trained in the use of a VPN?
- Does the user understand what is sensitive or valuable data and also who might wish to steal or acquire it?
- Is the user's physical location secure?
- Who has access to the user's location?

Secure Communication Channels – Data Communications

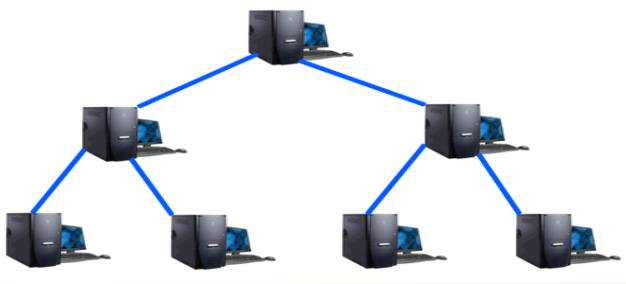
- Analog
- Digital
- Baseband (Ethernet)
- Broadband (cable TV)
- Synchronous Communication
- Asynchronous Communication

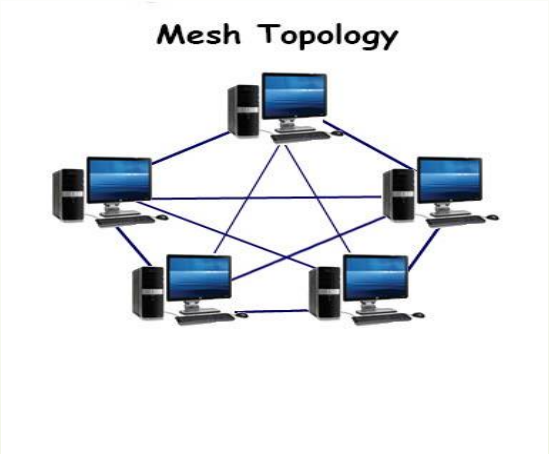


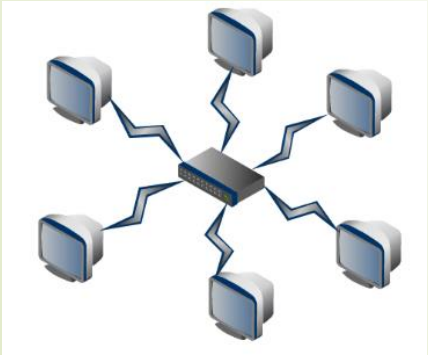
Secure Communication Channels – Data Communications

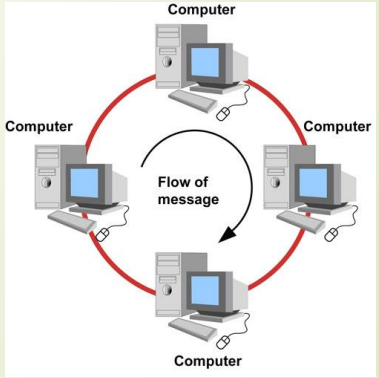


- Bus
- Tree
- Ring
- Mesh
- Star







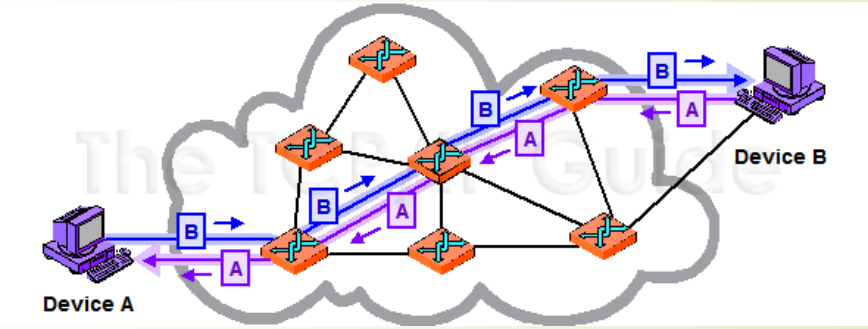


Secure Communication Channels – Data Communications

- Unicast
  - One to one (10.10.3.4 → 10.10.4.8)
- Multicast
  - One to many (or set, or group) 224.38.45.9
  - Controlled by group management protocols
- Broadcast
  - One to all (blocked by layer 3 routing devices)
  - 10.10.255.255
  - 255=all bits high (11111111)
- Anycast
  - One to one of many (unicast address assigned to a set of interfaces belonging to different nodes)

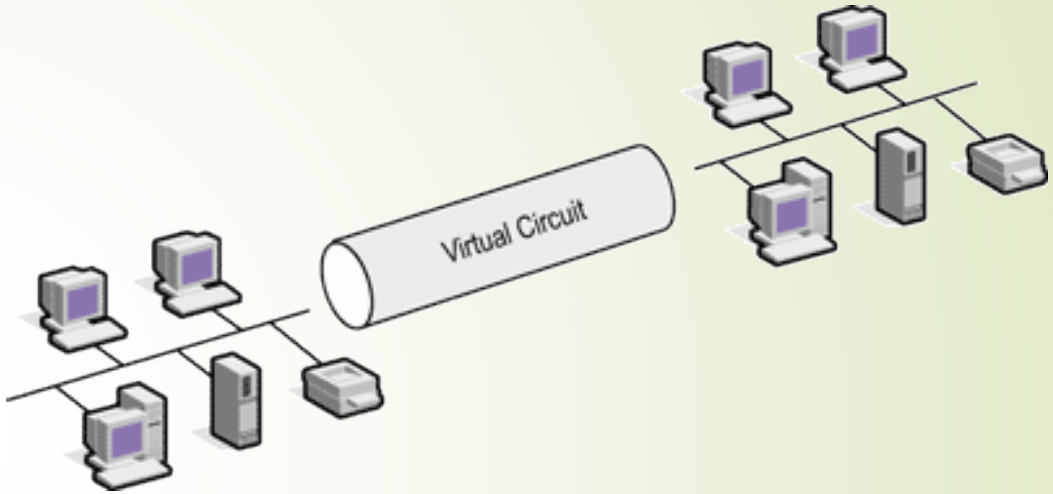
Secure Communication Channels – Data Communications

- Circuit Switched
  - Uses a fixed bandwidth and fixed path
  - Constant packet queues
    - No overhead bit-queuing



- Packet Switched
  - Splits data into packets
  - Static or variable sized
  - Each packet may take a different route (path) over a shared network
  - Emulates a circuit switched network by using virtual links

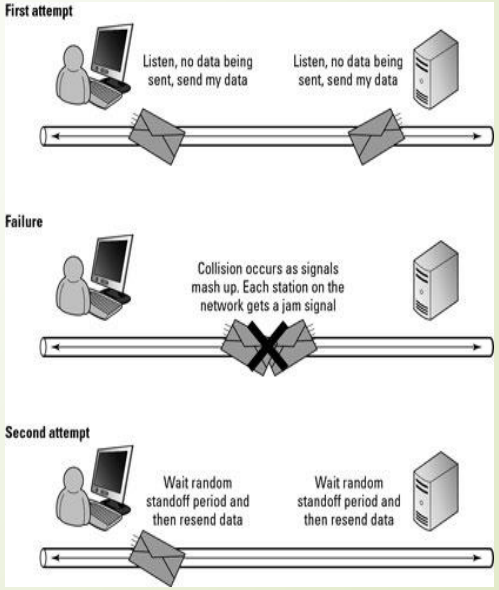
Secure Communication Channels – Data Communications



- Virtual Circuits Categories
  - Constant Bit Rate (CBR)
  - Variable Bit Rate (VBR)
  - Unspecified Bit Rate (UBR)
  - Available Bit Rate (ABR)
- Switched Virtual Circuit (SVC)
  - Virtual circuit switching (actually packet switched)
  - Established on demand
  - Maintains constant packet queues
    - Actual bit rate and latency are dependent on packet switched traffic load
- Permanent Virtual Circuit (PVC)
  - Dedicated circuit link (seldom disconnected)

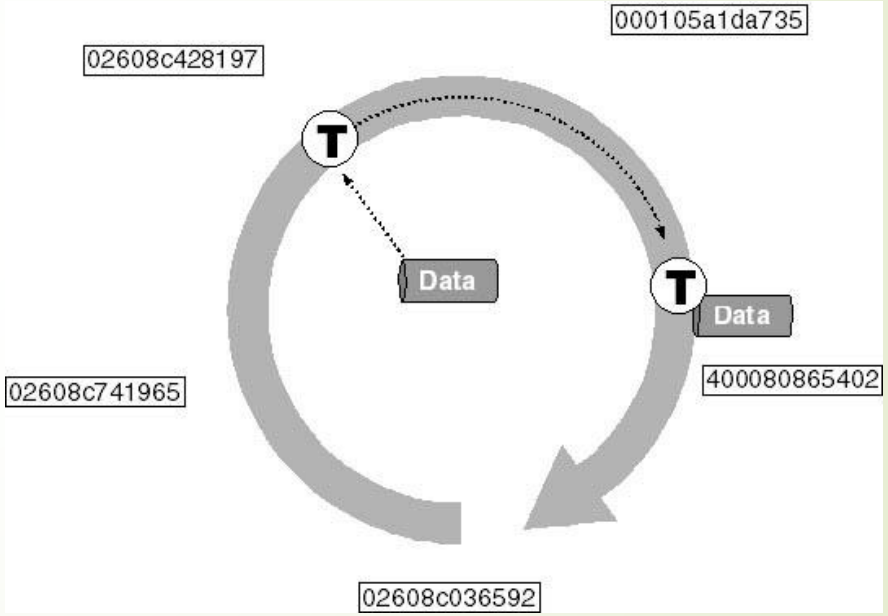
Secure Communication Channels – Data Communications

- Carrier Sense Multiple Access
  - Transmits when media is quiet
    - Uses a timeout period to detect collisions
- CSMA with Collision Avoidance (CSMA/CA)
  - Requests permission to transmit
  - Wireless method
- CSMA with Collision Detection (CSMA/CD)
  - Simultaneously transmits and listens for collisions
  - Hosts use hold-back timers to prevent another immediate collision



Secure Communication Channels – Data Communications

- Polling
  - Mainframe protocol
  - Option on IEEE 802.11
- Token passing
  - One transmission at one time

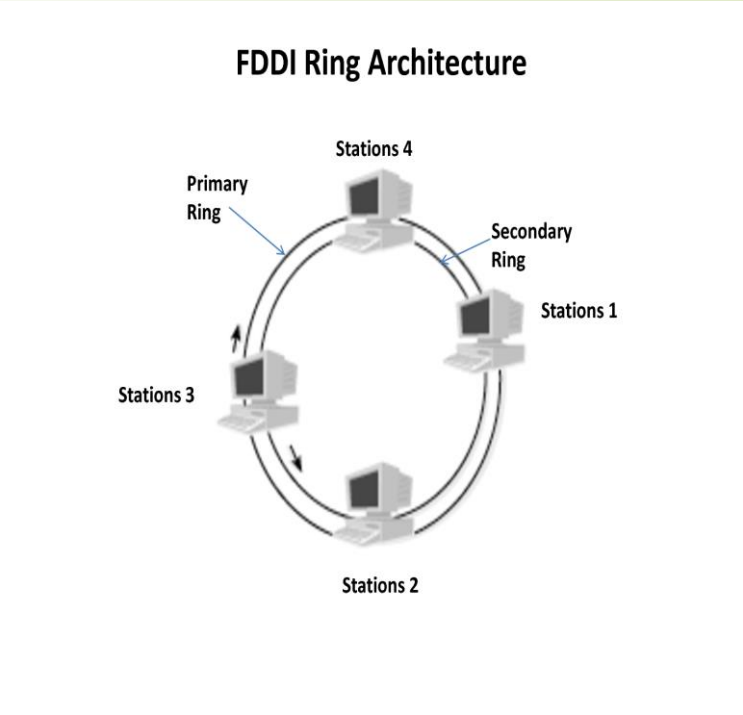


Secure Communication Channels – Data Communications

- Ethernet (802.3)
  - Ethernet (10Mb)
  - Fast Ethernet (100Mb)
  - Gigabit Ethernet (1000Mb)
- 10 Gigabit Ethernet (10GbE)
- Future Standards
  - 40 Gigabit Ethernet (40GbE)
  - 100 Gigabit Ethernet (100GbE)

Secure Communication Channels – Data Communications

- Token Ring (802.5)
  - Token travels in a logical ring
    - Hosts "poll" for token (transmission) availa
    - Standard 16Mbps
    - Full Duplex Token Ring 32 Mbps
- Fiber Distributed Data Interface (FDDI)
  - 802.4 token-bus based, also used in MANs
  - Employs dual rings
    - Traffic flows in opposite directions on each
    - Was also used as a WAN technology

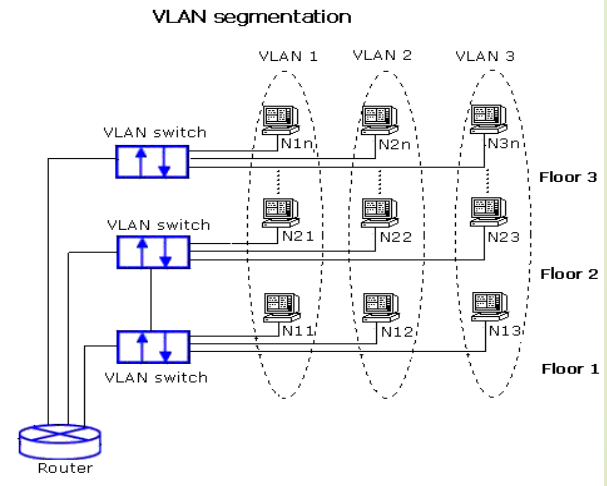


Secure Communication Channels – Data Communications

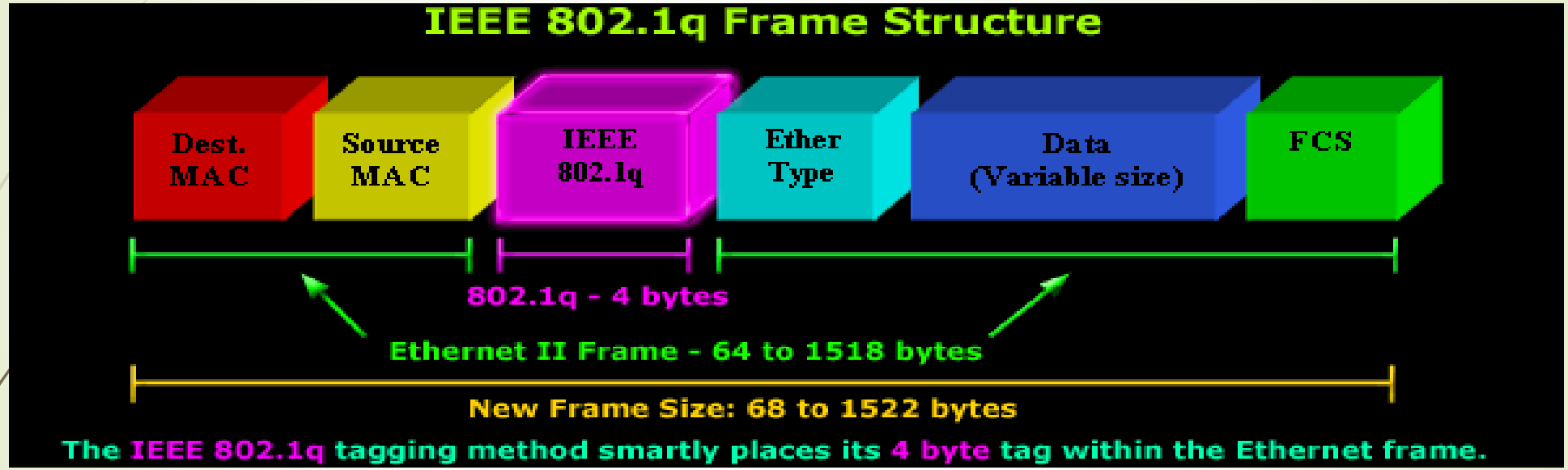
- Transport security (IPSec, TLS, SSL)
- Trunking security
  - VLANs
    - VLAN Hopping (use one VLAN to access another)
    - 802.1Q

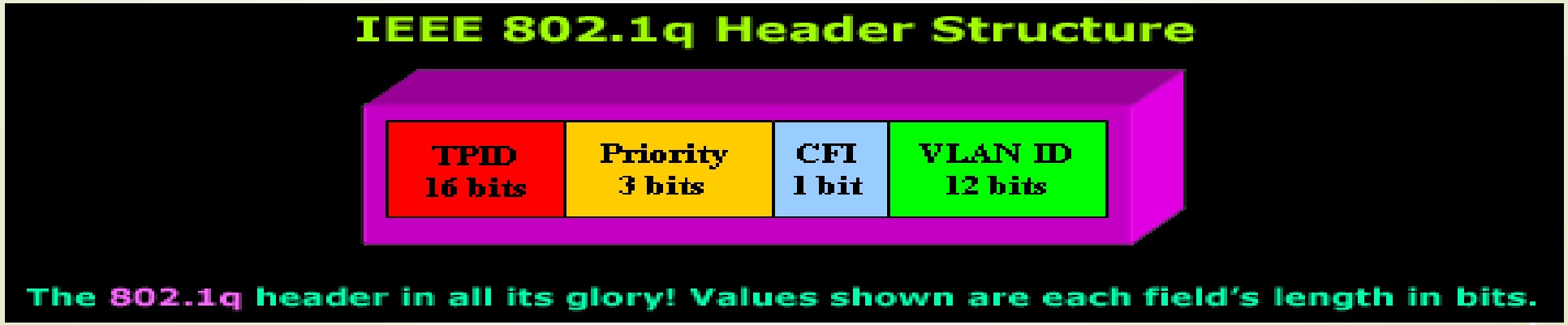
Secure Communication Channels – Data Communications

- Virtual Local Area Networks (VLANs)
  - Divides the broadcast domain into a number of VLANs
  - Attacks
    - MAC Flooding Attack
    - 802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack
    - Double Encapsulated 802.1Q/Nested VLAN Attack
    - ARP attacks
    - Multicast Brute Force Attack
    - Spanning Tree Attack
    - Random Frame Stress Attack



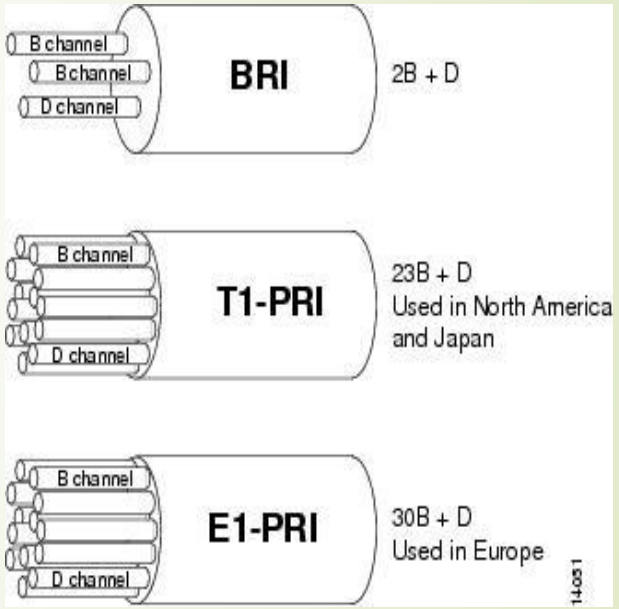
IEEE 802.1Q Frame Structure





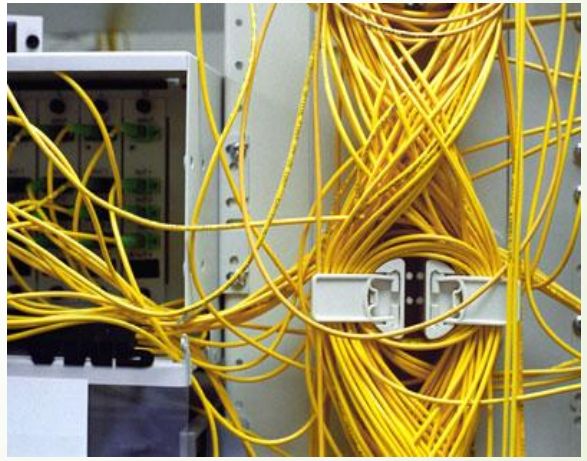
Secure Communication Channels – Data Communications

- Integrated Services Digital Network (ISDN)
  - BRI (One 16Kbps D channel, Two 64Kbps B channels)
  - PRI (One 64Kbps D channel, Twenty Three 64Kbps B channels)
    - In Europe, One D channel, Thirty B channels
    - Commonly used in PBXs
  - D-Channels: Call setup/maintenance
  - B-Channels: Carry network payload



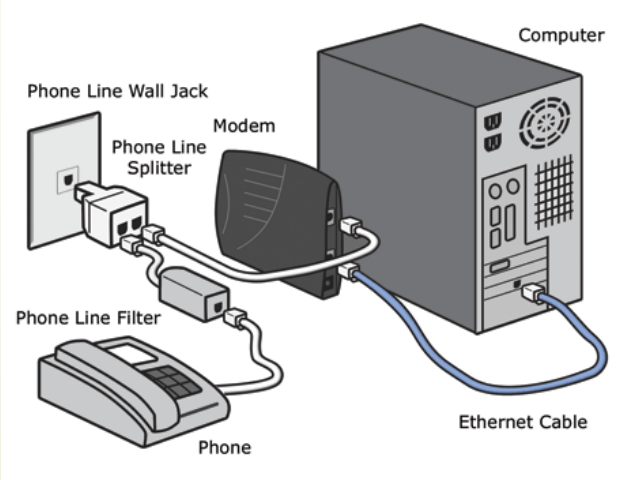
Telecommunication Circuit Technologies

- T, E, J, and O Carriers
  - T = Copper Carrier
    - T1 = 1.544 Mbit/s
    - T3 = 44.736 Mbit/s
  - E = Copper Carrier
    - E1 = 2.048 Mbit/s
    - E3 = 34.368 Mbit/s
  - J = Copper Carrier
    - J1 = 1.544 Mbit/s
    - J3 = 32.064 Mbit/s
- O = Optical Carrier (SONET)
  - OC-1 = 50 Mbit/s payload
    - OC-n = n x 51.8 Mbit/s



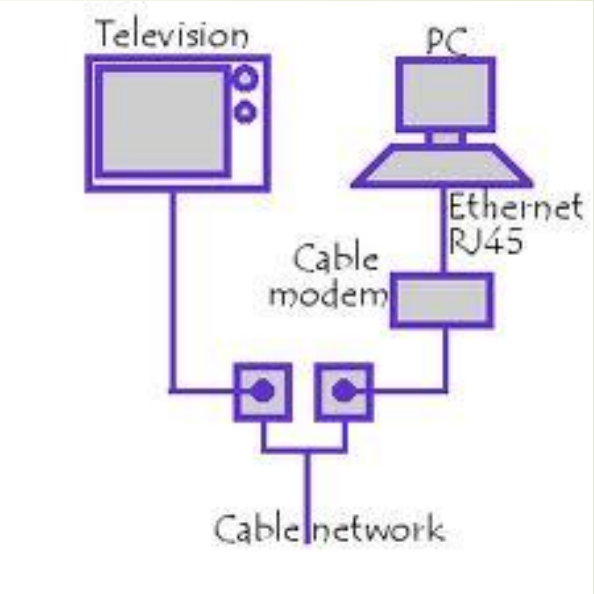
Secure Communication Channels – Data Communications

- Digital Subscriber Line (DSL)
  - Uses existing phone lines
  - DSL modem separates voice and data
    - Communicates with central office DSLAM
      - Must be within 18,000 ft
- Different Variations
  - ADSL
  - SDSL
  - HDSL
  - VDSL
  - RADSL



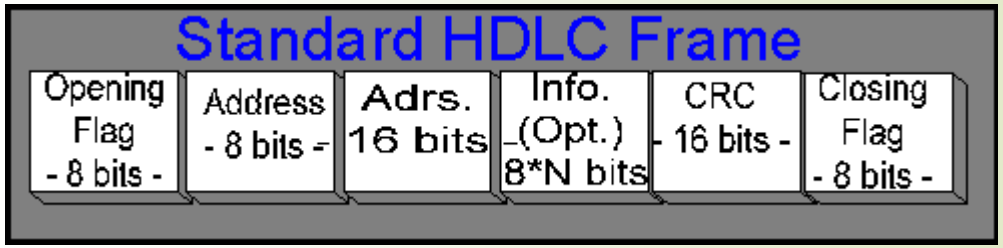
Secure Communication Channels – Data Communications

- Cable Modem
  - Uses existing Cable TV coax medium
  - DOCSIS
    - Data Over Cable Service Interface Specification
    - Modern DOCSIS provides 56-bit DES and 128-bit AES
  - Cable modem separates video and data
    - Sent to cable modem termination system (CMTS) at headend



Secure Communication Channels – Data Communications

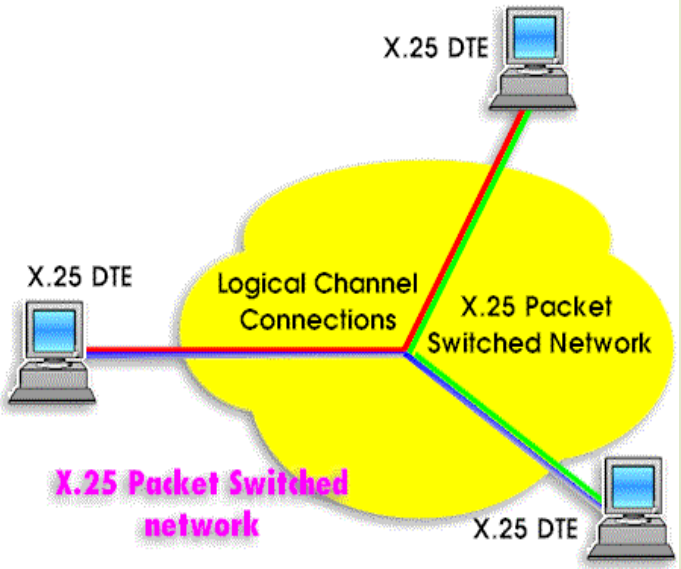
- Synchronous Data Link Control (SDLC)
  - Layer 2
  - Uses polling similar to token ring



- High-Level Data Link Control (HDLC)
  - Successor to SDLC
  - Added error correction and flow control
  - 3 modes
    - Normal Response Mode (NRM)
    - Asynchronous Response Mode (ARM)
    - Asynchronous Balanced Mode (ABM)

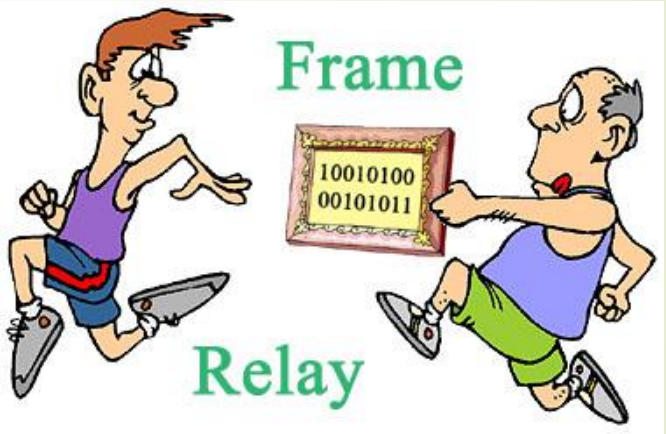
Secure Communication Channels – Data Communications

- X.25 (1980s) (Europe, X.25WAN – modern)
  - Supports SVC and PVC (except older providers)
  - Packet Switched
  - LAPB=HDLC in Asynchronous Balanced Mode
    - Slower (due to analog properties and built-in error correction)



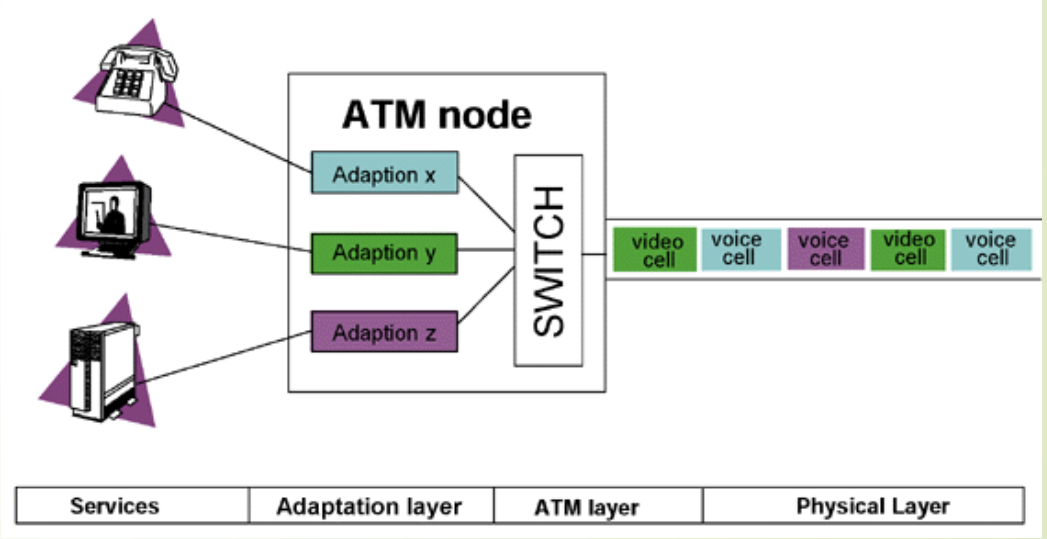
Secure Communication Channels – Data Communications

- Frame Relay
  - Replaced many X.25 circuits
  - Also Packet Switched
  - DCE/DTE (commonly a HSSI Interface)
  - No error recovery and focuses on speed
  - Initially designed for T1+ carriers
    - Uses a variable sized frame
    - Committed Information Rate (CIR)
    - Can "burst" into neighbors bandwidth, providing they are not currently using it



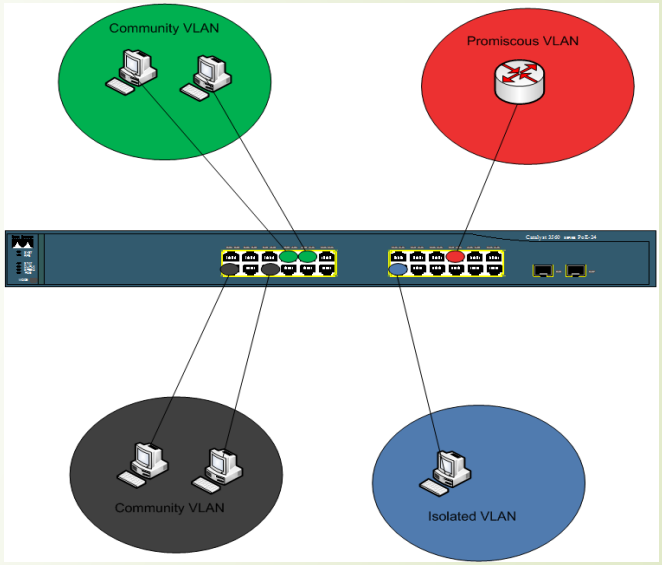
Secure Communication Channels – Data Communications

- Asynchronous Transfer Mode (ATM) (cell switching, Broadband ISDN)
  - Provides both SVC and PVC
  - Fixed size frame, 53-byte cells
    - Reduces jitter, good for voice
  - Initially designed for T3+ carriers



Secure Communication Channels – Data Communications

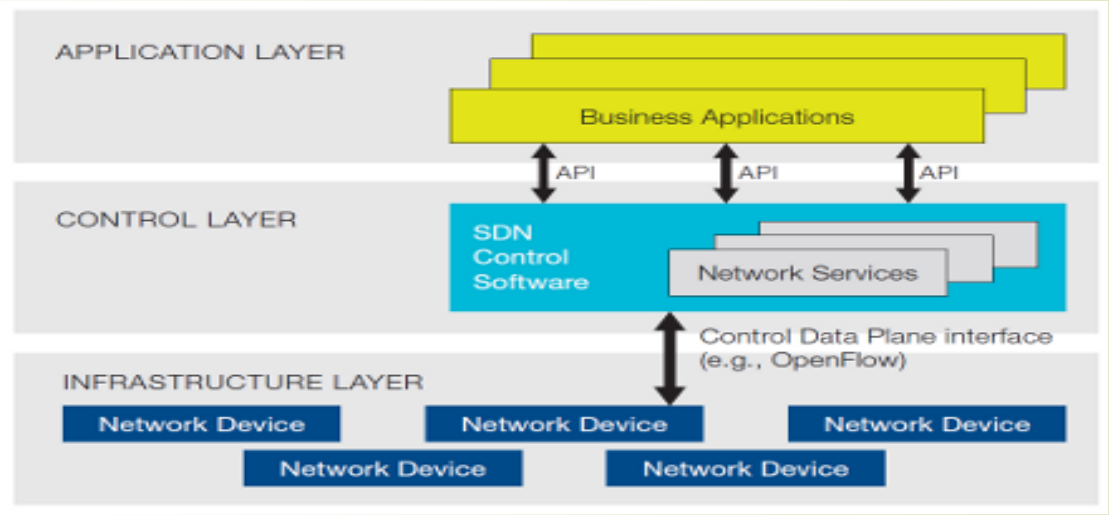
- Virtualized Networks
  - Software Defined Networking (SDN)
  - Software Defined Storage and Virtual SAN (SDS)
  - PVLANs, Virtual Networks, and Guest Operating Systems



Virtualized Networks - Software Defined Networking (SDN)

- Control and data plane are decoupled
- Network intelligence and state are logically centralized
- Network infrastructure is abstracted from the application
- Purpose: to separate traditional network traffic into three components
  - Raw data
  - How data is sent
  - What purpose the data serves

Virtualized Networks - SDN

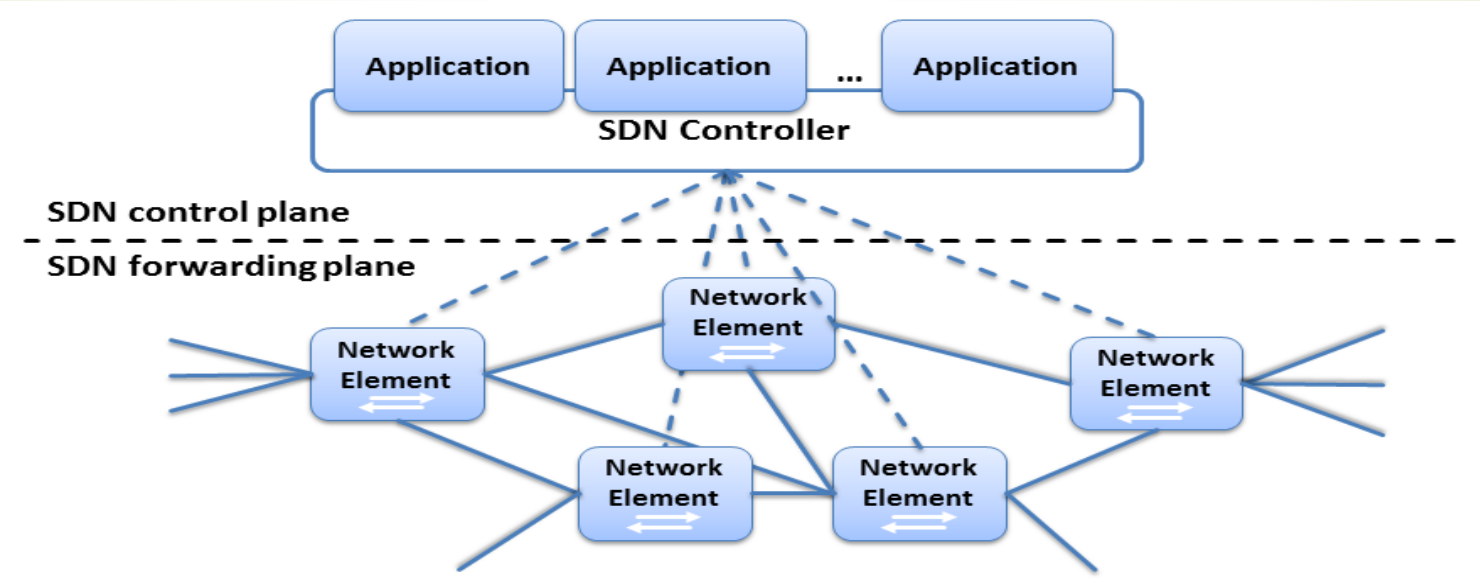


Three Layers

- Infrastructure Layer (data plane)
  - Switches, routers, and data
- Control Layer (control plane)
  - Intelligence in the devices (how data should flow)
- Application Layer (application plane)
  - Network services, utilities, and applications that interface with the control layer

Virtualized Networks - SDN

- Cloud and Virtualization have the potential to benefit the most
- Based upon open standards such as OpenFlow



Virtualized Networks - SDN Architectural Components

- **SDN Application (SDN App)**
- **SDN Controller**
- **SDN Datapath**
- **SDN Control to Data-Place Interface (CDPI)**
- **SDN Northbound Interfaces (NBI)**

Virtualized Networks - Southbound Defined Storage and Virtual SAN (SDS)

- **Aka Software defined storage (SDS)**
- **Definition: any software storage stack that can be installed on any commodity resource (x86, hardware, hypervisors, or cloud) and off-the-shelf computing hardware**
- **In a software defined data center (SDDC) all services are built on the virtualization layer which decouples the data and control planes but allows storage functionality**

Traditional Enterprise Storage Services

- Dynamic Tiering: shifting data between tiers (flash/hard drives)
- Caching: flash storage
- Replication: storage replication and data protection
- Quality of Service (QoS): predictable, consistent, high performance
- Snapshots: point in time copy
- Deduplication: reduce capacity requirements (block level)
- Compression: crunch files down to fraction of original size (file level)
- Cloning: improves overall service

Virtualized Networks - SDS Protection & Data Availability Mechanisms

- **Intelligent data placement**
- **Controllers**
- **Software RAID**
  - **Makes hardware based RAID systems unnecessary**

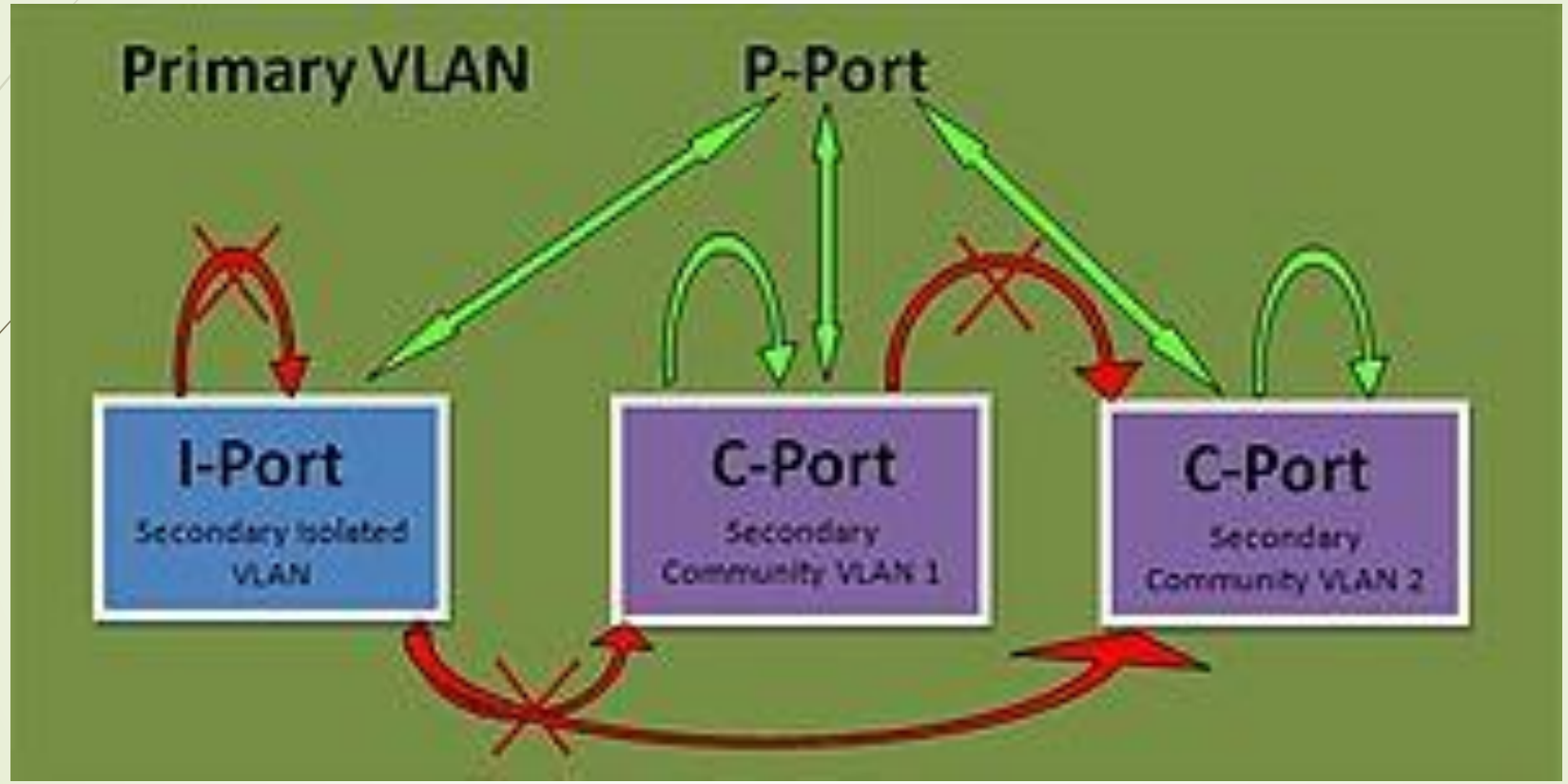
Virtualized Networks - Virtual SAN

- Hypervisor-Converged Storage
- VM-Centric Policy-Based Management and Automation
- Server-Side Read/Write Caching
- Built-in Failure Tolerance
- Granular Non-Disruptive Scale-Up and Scale-Out
- Hardware Independent

Virtualized Networks - PVLANs

- Private VLANs allow traffic to be separated at another level allowing for a number of flexible options for design and security
- Divided into groups
- Primary PVLAN
  - Original VLAN (secondary PVLAN exist in the primary)
- Secondary PVLAN
  - Promiscuous (port): send/receive packets to any other secondary PVLAN (routers)
  - Isolated (port): only send/receive packets from promiscuous PVLAN
  - Community (port): send/receive from same secondary PVLAN and send/receive packets from promiscuous PVLAN

Virtualized Networks - PVLANs



Network Attacks

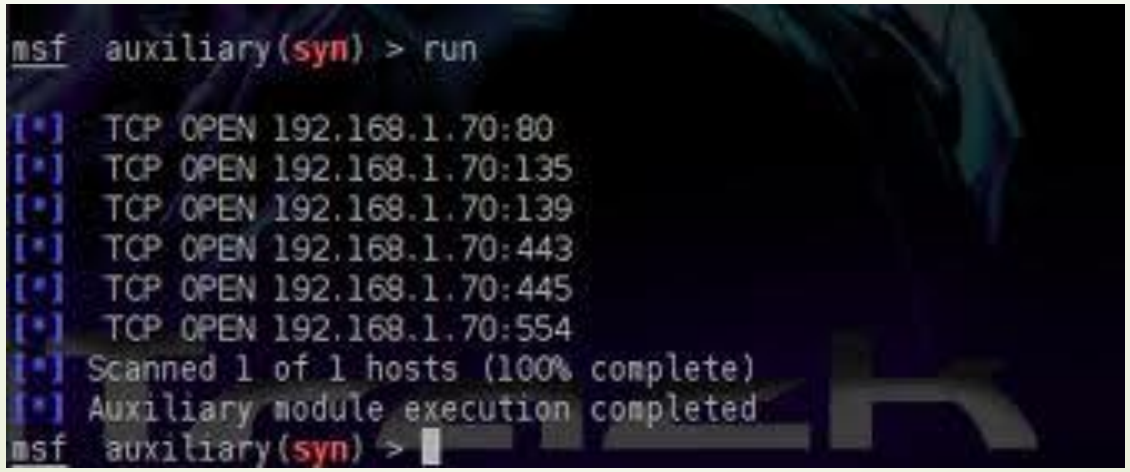
- The network as a target of attack
  - IP Convergence
- The network as an enabler or channel of attack
- The network as a Bastion of defense
- Threat Vectors:
  - External threat against Bastian hosts (web, mail, SMTP), internal servers, and internal clients
  - Internal threat against internal servers, clients, and infrastructure

Network Attacks - Scanning Techniques

- ARP
- ICMP
- UDP Port scanning
- TCP Port scanning
  - SYN/FIN/NULL and XMAS scanning

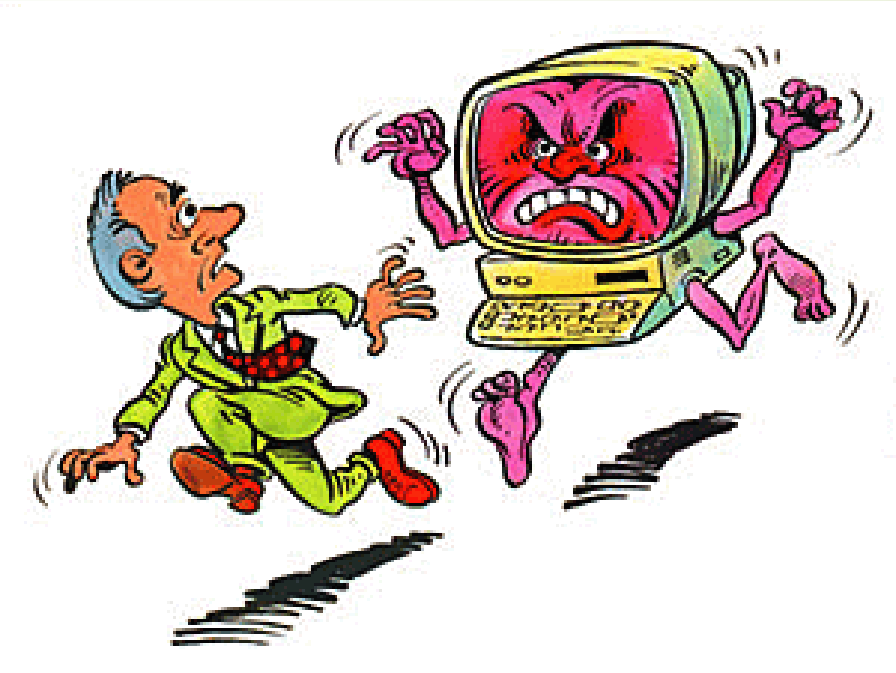
Scanning - Stealth (SYN) Scan

- SYN scanning is a type of stealth scan that makes use of SYN packets
- Aka half-open scanning / TCP SYN Scanning
- Doesn't finish the TCP 3 way handshake



Network Attacks - Methodology of an attack

- Target acquisition
- Target analysis
- Target access
- Target appropriation



Network Attacks - Attackers

- Hackers
- Black/White Hats
- Script Kiddies
- Outsiders
- Insiders
- Hacktivist
- Bots and Botnets
- Phishers and Spear Phishers

Network Attacks - Password Attacks

- Guessing
- Dictionary Attack
- Social Engineering
- Countermeasures:
  - User Training
  - Use etc/shadow vs. etc/passwd
  - Clipping Levels

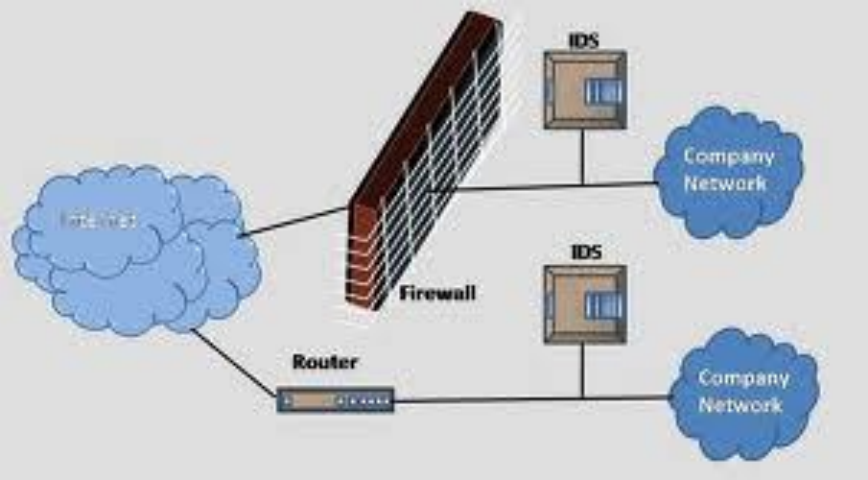
Network Attacks - Social Engineering

- Methods
  - Lying
  - Bullying and Intimidation
  - Dumpster Diving
  - Shoulder Surfing
  - Phishing

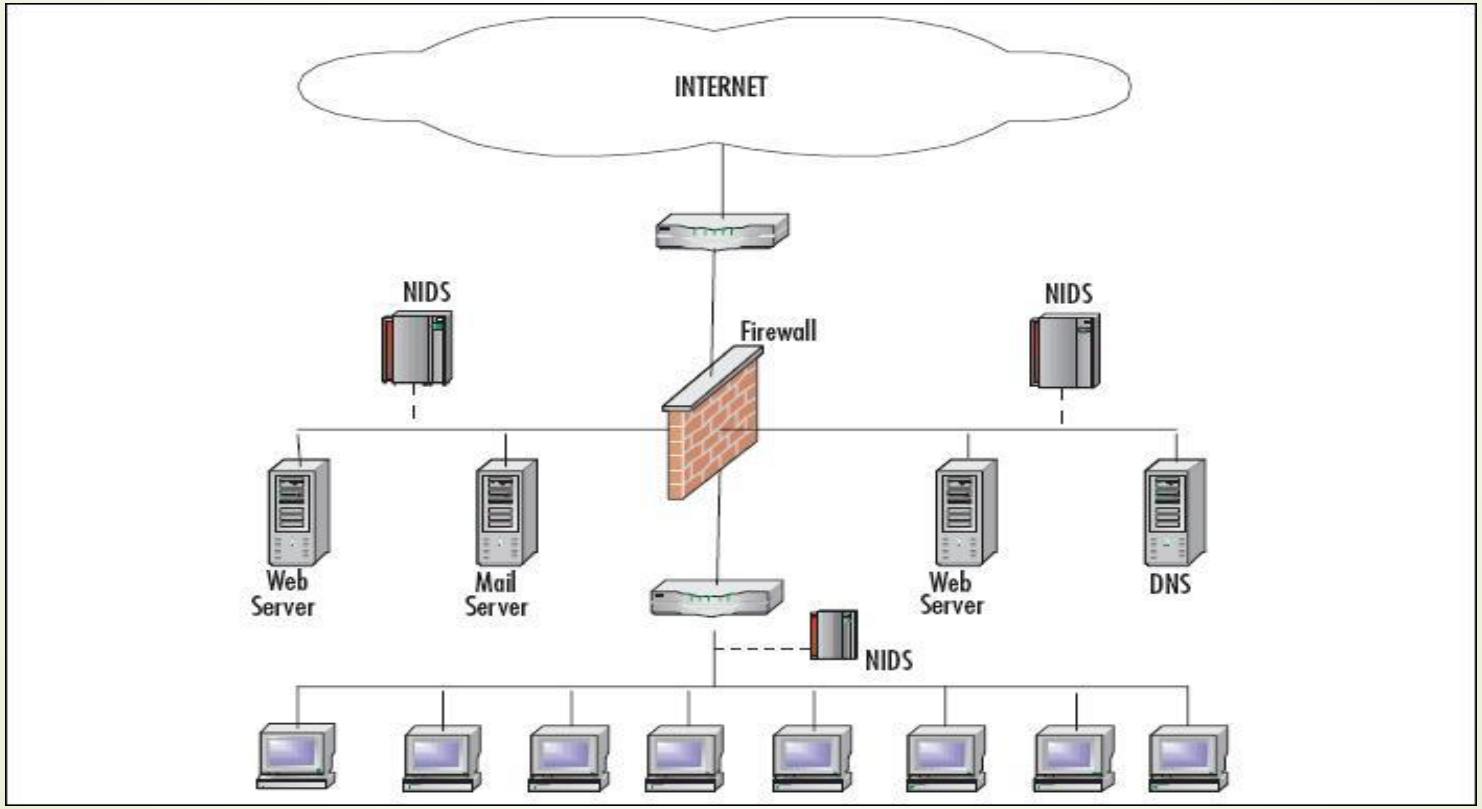
- User awareness is your best weapon to fight social engineering

Network Attacks – Network Security Tools and Tasks

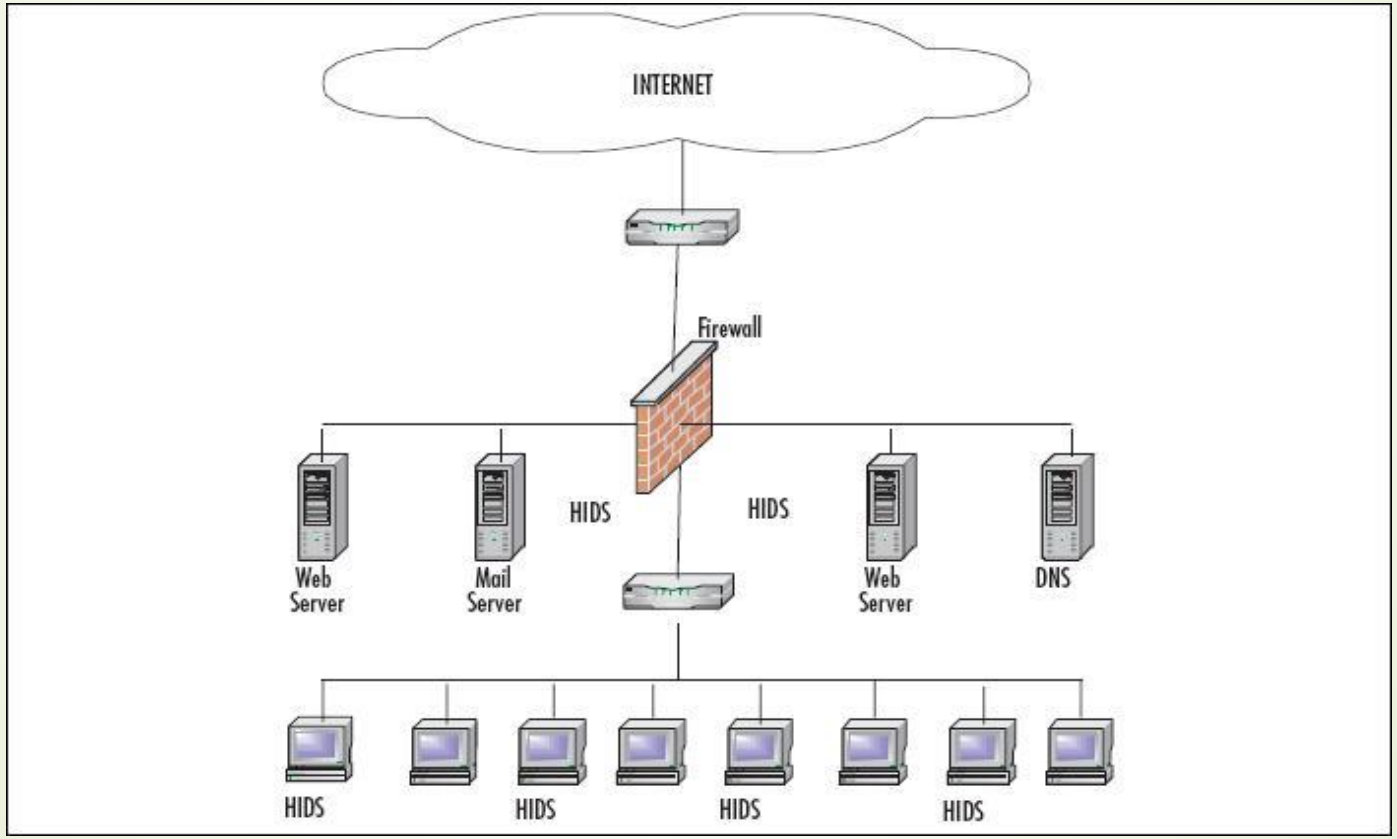
- Intrusion Detection Systems (IDS)
  - Monitor activity and send alerts when suspicious activity is detected
  - 2 Types of IDS
    - Host based IDS
    - Network based IDS
  - 2 ways to detect
    - Signature based
    - Heuristic (anomaly) based



Network Security Tools - Network Based IDS (NIDS)



Network Security Tools - Host Based IDS (HIDS)



IDS & IPS - Functionality

- Detects attacks from outside your organization
- Detects misuse and attacks from within
- Uses known patterns (signatures), heuristics or anomaly detection
- Alerts administrators to intrusion attempt
- Disconnects the attacker from resources

IDS & IPS - Event Types

- **False Positives - accepted activity identified as malicious activity**
- **False Negatives - malicious activity that is not reported**
- **True Positives – malicious activity identified as malicious activity**
- **True Negative – normal traffic identified as normal traffic**

IDS/IPS - Response Types

- Passive
- A passive IDS looks for security breaches, but effectively takes no action
- It is the network administrator's job to interpret the degree of the threat and to respond accordingly
- Types of activities:
  - Logs suspicious activity
  - Generates alerts if the attack is deemed to be severe

IDS/IPS - Response Types

- Active
- An active IDS can be configured to take specific actions when security breaches occur
- Types of activities:
  - Dynamically adjusts policy and reconfigure a network devices
  - Updates filters
  - Performs reverse lookups

IDS & IPS - Intrusion Response Capabilities

- IDS/IPS response capabilities include:
  - Dropping suspicious data packets at firewall
  - Denying access to a user displaying suspicious activity
  - Reporting the activity to other hosts on site
  - Updating configurations within the IDS

IDS - Methods

- Signature-Based Detection
- Anomaly-Based Detection
- Stateful Matching Intrusion Detection
- Statistical Anomaly-Based Intrusion Detection
- Protocol Anomaly-Based Intrusion Detection
- Traffic Anomaly-Based Intrusion Detection

Network Attacks – Security Event Management

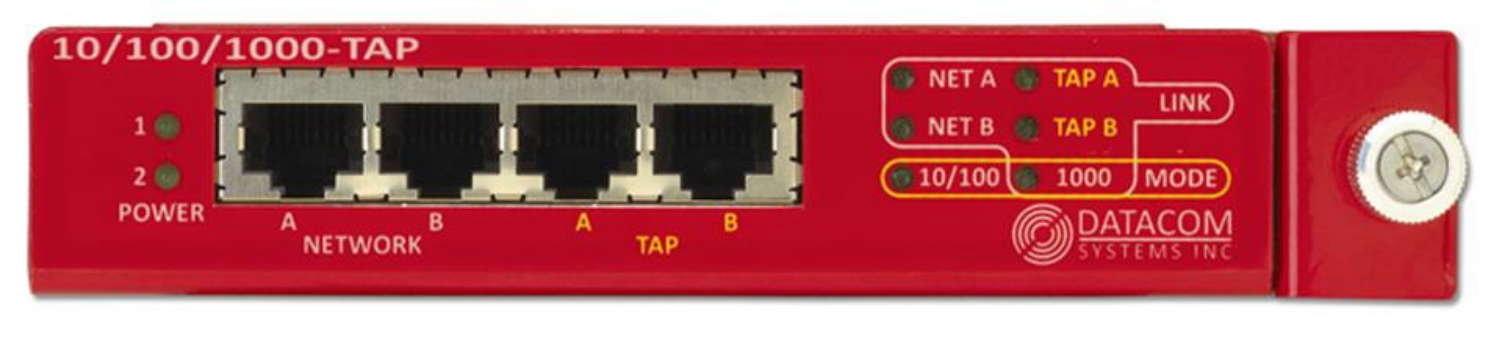
- Vulnerability Management is not just vulnerability scanning but also the managing of the scanning process and the prioritization and remediation of the vulnerabilities
- Vulnerability Scanning
  - Eye-Retina, OVAL, Nessus, SAINT, SATAN, GFI Languard, etc
- Zero day vulnerabilities
  - Vulnerability known before a patch is created
- Zero day exploits
  - Exploit available prior to a patch being developed

Network Attacks – Security Event Management

- **Vulnerability Scanning**
  - **Conducted against network, host system, and application resources**
  - **Identify policy and security configuration vulnerabilities**

Network Attacks - Network Taps

- Network Taps
  - Provides promiscuous access to a network
- Span Ports
  - Switched Port Analyzer (SPAN)
  - Mirror traffic from multiple ports to one span port
  - Traffic may exceed capability of port

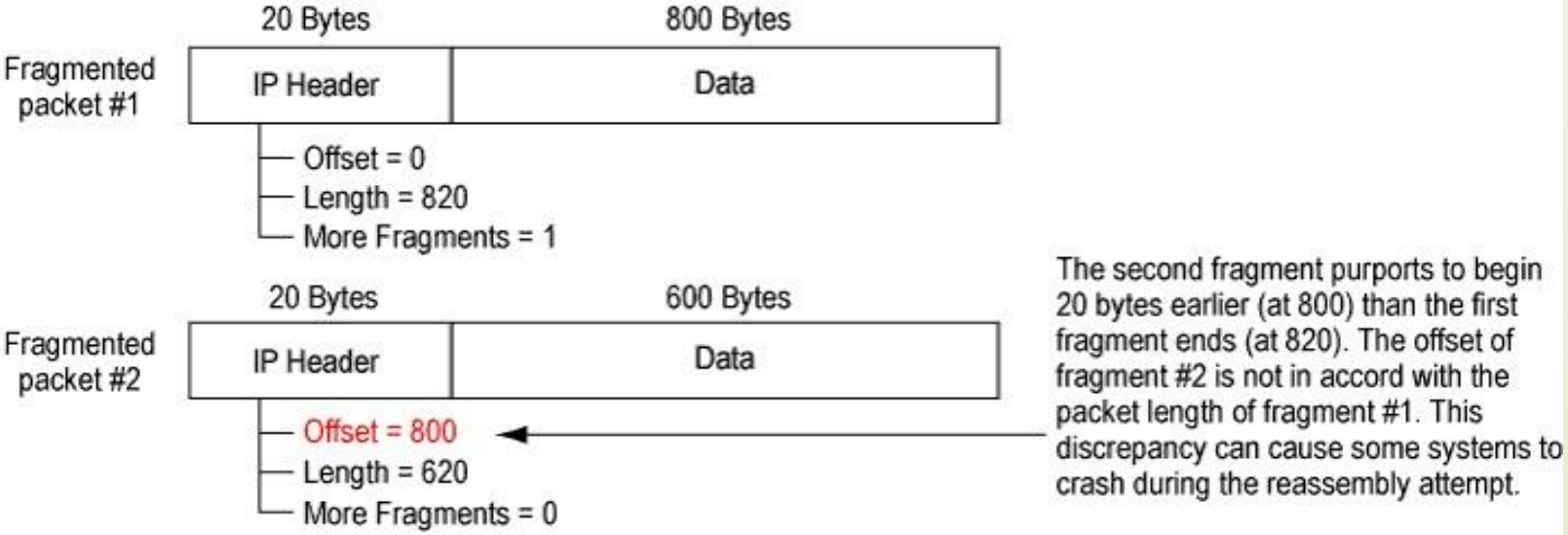


Network Attacks – IP Fragmentation Attacks & Crafted Packets

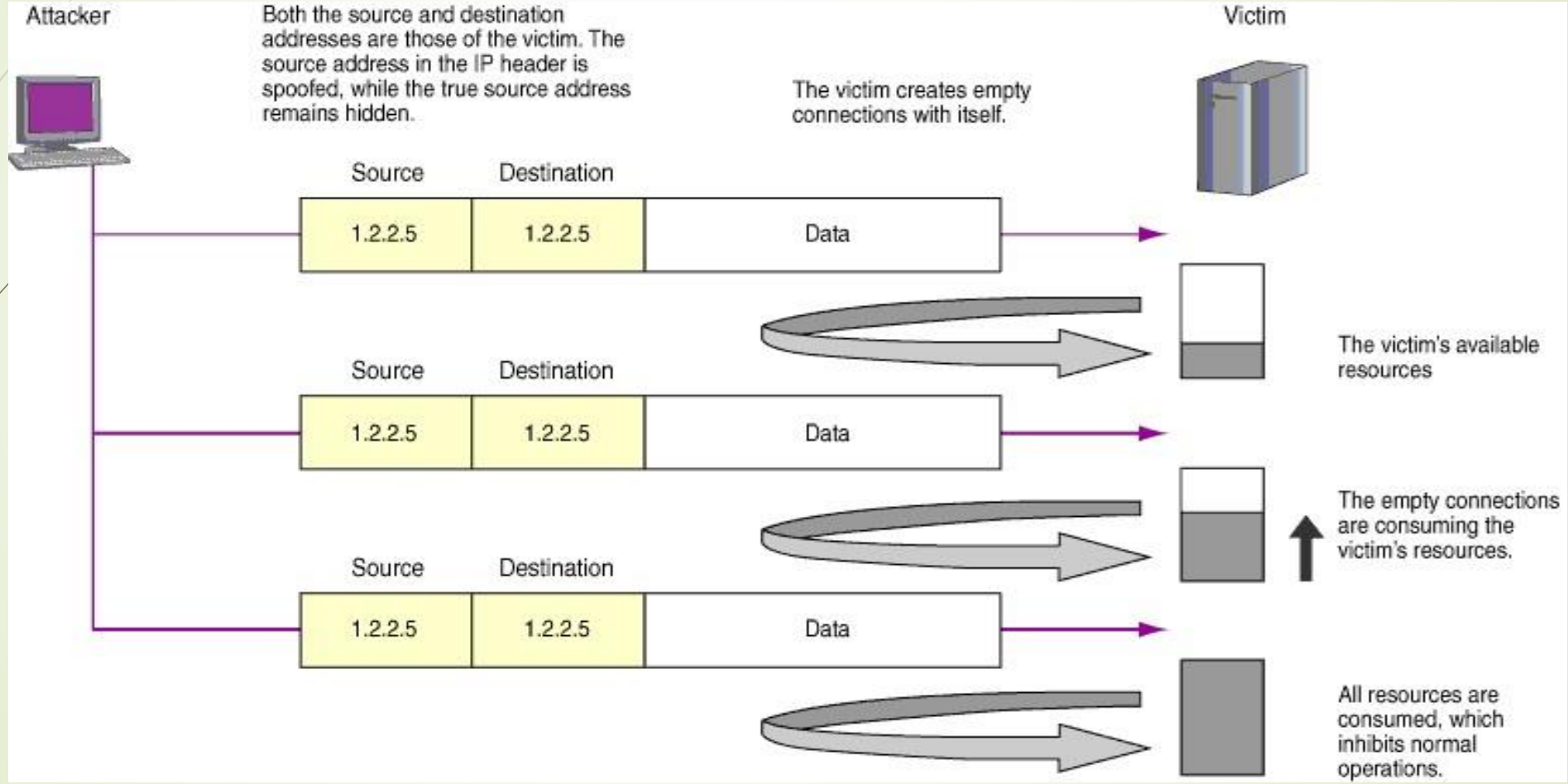
- Teardrop
- LAND attack
- Smurf
- Fraggle
- TCP SYN flooding
- Sequence Number attacks
- Session Hijacking

IP Fragmentation Attacks & Crafted Packets - Teardrop

- **IP Fragmentation and crafted packets**
- **Sends overlapping packet fragments in which TCP/IP cannot handle**

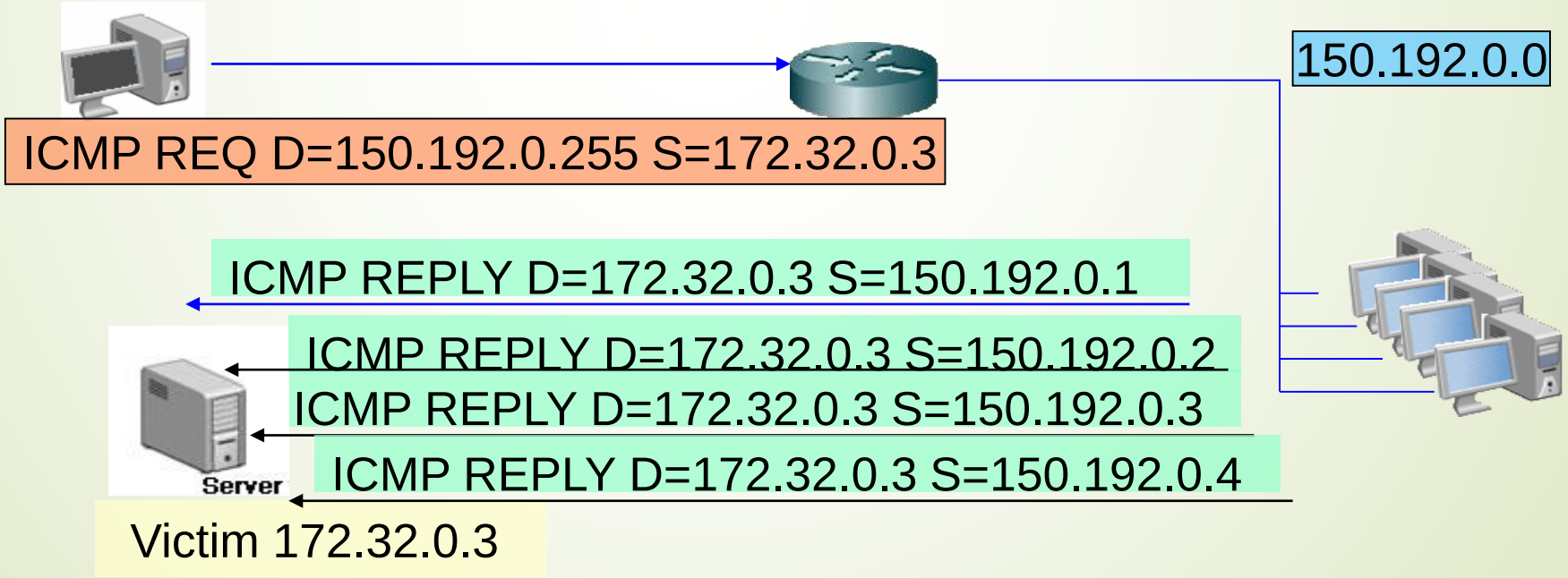


IP Fragmentation Attacks & Crafted Packets - LAND Attacks

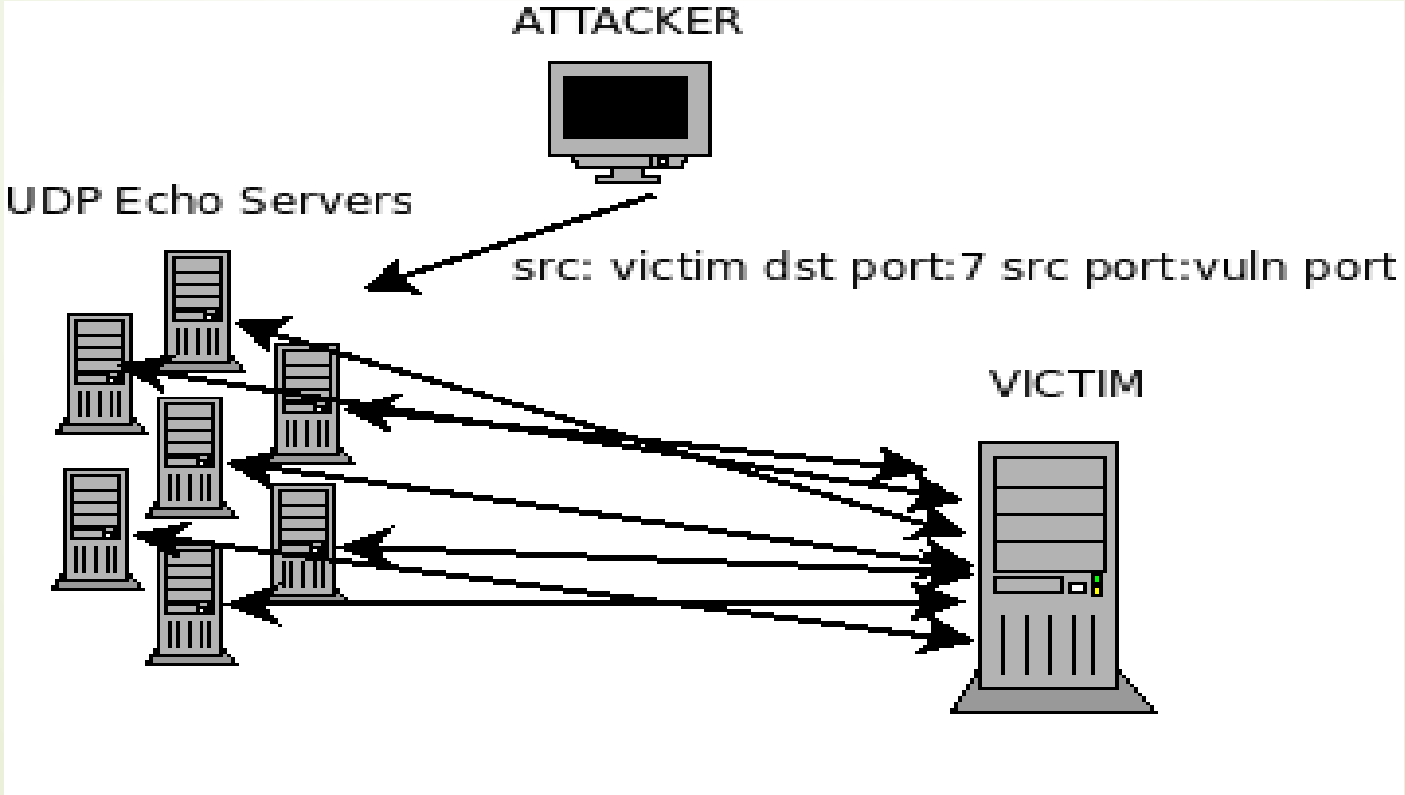


IP Fragmentation Attacks & Crafted Packets - SMURF

- **Attacker sends multiple IP ping requests to a receiving device (typically via a router)**



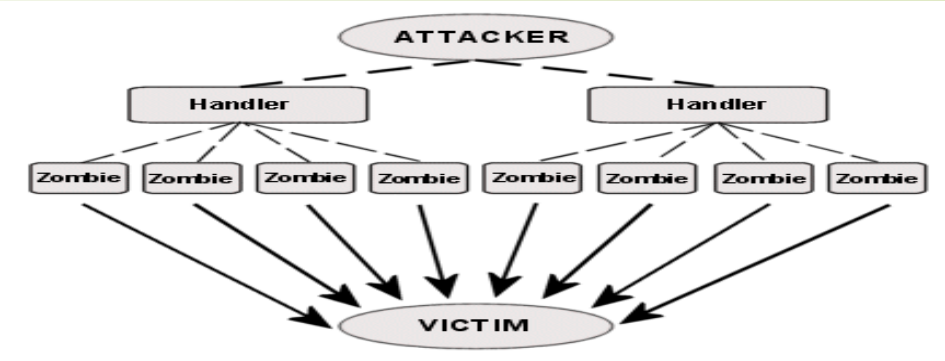
IP Fragmentation Attacks & Crafted Packets - FRAGGLE



Network Attacks – DoS & DDoS Attacks

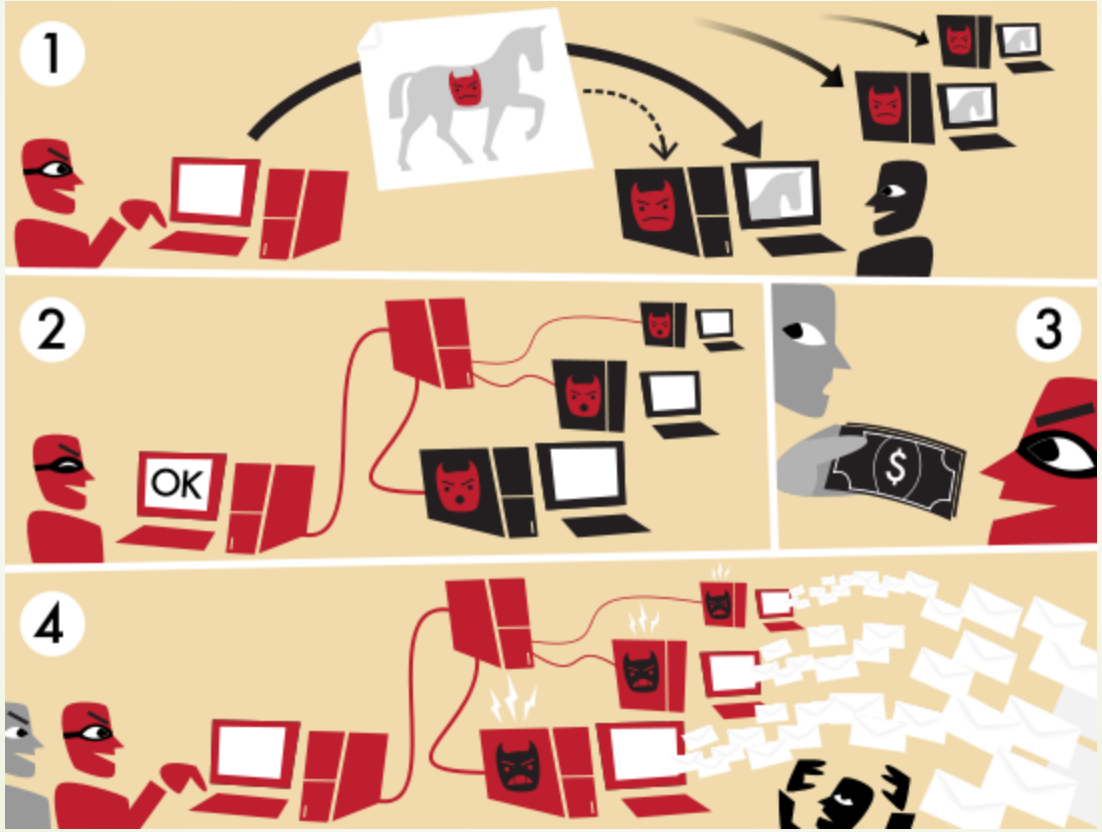
- **Denial of Service (DoS) Attack**
  - **Attempts to prevent legitimate users from accessing information services**
- **Distributed Denial of Service (DDoS) Attack**
  - **Amplifies a DoS by using multiple computers to conduct an attack against a single entity (Smurf Attack)**
  - **Compromised systems are referred to as Bots or Zombies**

DDoS - Components

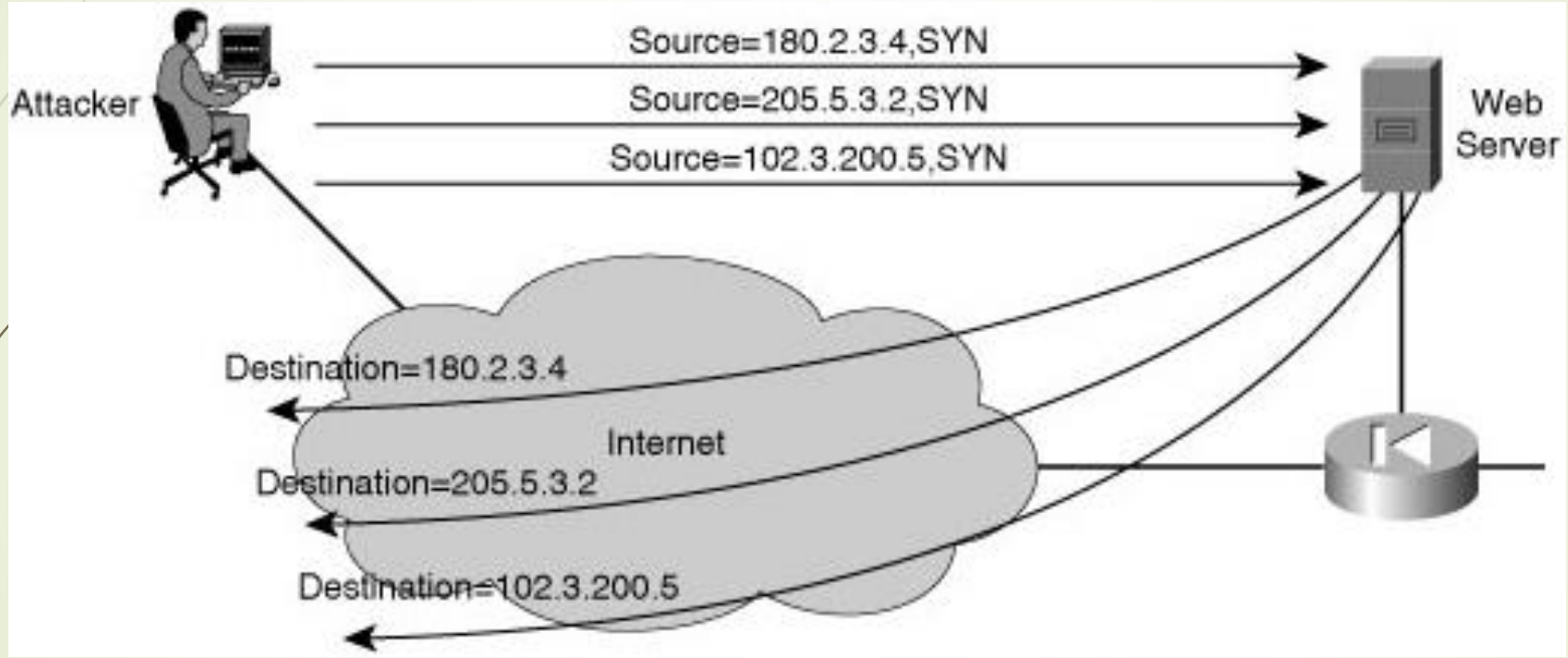


- Zombies
  - A computer compromised by a hacker that is used to perform malicious tasks under remote direction
- Botnets
  - A network of compromised systems containing malware which acts as a robot
  - Bots are programs that run automated tasks
    - Obeys a master or author of the code

DDoS Attack - Spammer Botnet



DoS Attack - TCP SYN Flooding



Network Attacks – Session Hijacking

- Act of unauthorized insertion of packet into a data stream
  - MITM
  - Communications intercepted between an authorized user and resource
  - Attacker takes over the session and assumes the identity of the authorized user

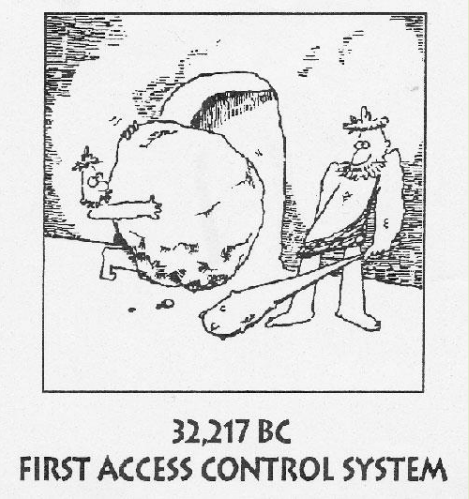
Questions?

Identity and Access Management

(Controlling Access and Managing Identity)

Domain Objectives

- Control physical and logical access to assets
- Manage identification and authentication of people and devices
- Integrate identity as a service
- Integrate third-party identity services
- Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle



Physical & Logical Access to Assets - Access Control

- **The process of allowing only authorized users, programs, or other computer systems (i.e. networks) to observe, modify or otherwise take possession of the resources of a computer system. It is also a mechanism for limiting the use of some resources to authorized users.**

Physical & Logical Access to Assets - Access Control Concepts

- **Access Controls – A collection of mechanisms, that work together to protect the assets of an enterprise**
  - **Protects against threats and vulnerabilities by reducing exposure to unauthorized activities**
  - **Only allows access to information systems that have been approved**
  - **Implements an auditable trail that provides non-repudiation of object access**

Physical & Logical Access to Assets - Access Control Policy Elements

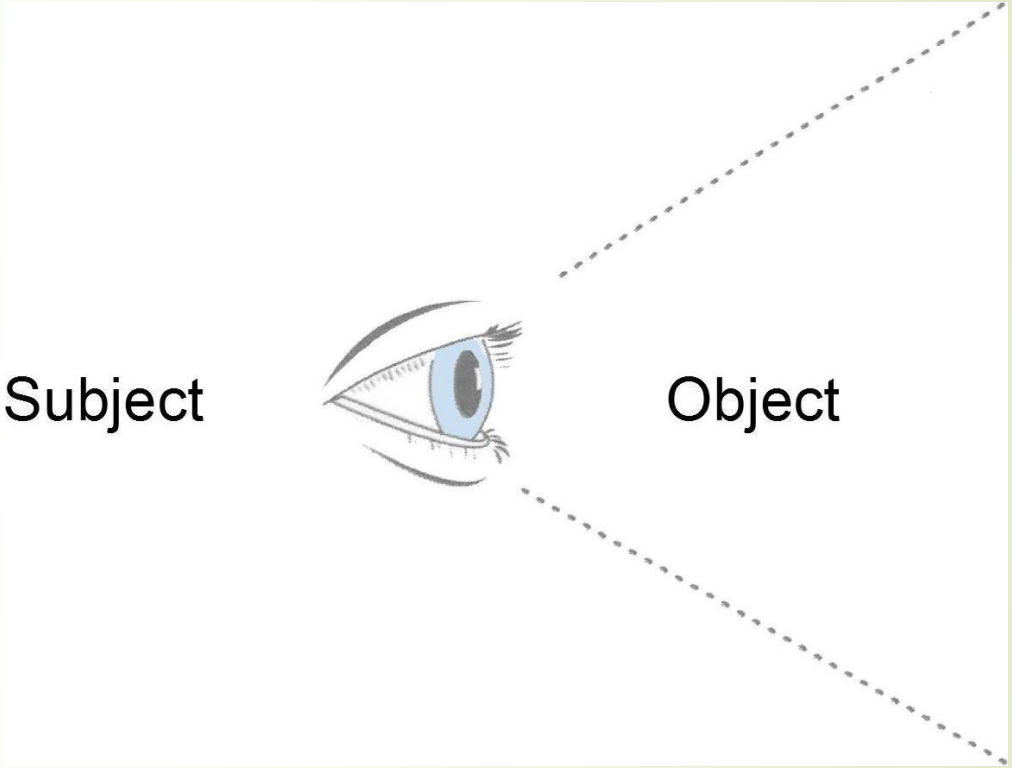
- Statements of general security principles and applicability to the organization
- Security requirements of individual enterprise applications, systems and services
- Consistency between the access control and information classification policies of different systems and networks
- Contractual obligations or regulatory compliance
- Standards defining user access profiles or roles
- Details regarding the management of the access control system

Physical & Logical Access to Assets - Access Control Process

- **Define Resources**
- **Determine Users**
- **Specify Use**

Subjects and Objects

- **Subject**
  - **The active entity on the network**
- **Object**
  - **The passive entity on the network**



Physical & Logical Access to Assets - Physical Access Control Systems (PACS)

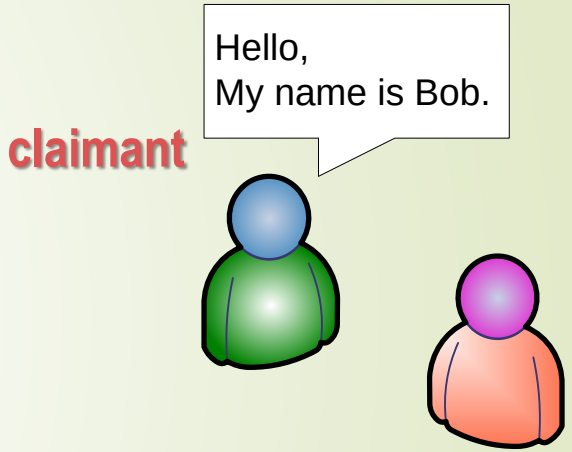
- **Allow security personnel to simultaneously manage and monitor multiple entry points from a centralized location.**
- **Can be divided into 4 areas:**
  - **Identification**
  - **Visitor management**
  - **Parking permit management**
  - **Alarm monitoring and intrusion detection**

Identification & Authentication of People & Devices

- The control environment must provide access controls to systems, data and resources. Access to data and resources are concerned with:
  - Identification – Who is the subject
  - Authentication – Verification of the subject
  - Authorization – What a subject can do
  - Accounting – What a subject has done
  - Auditing – Proof of Non-Repudiation
  - Availability – Ensuring the object is available to subject

Identification & Authentication of People & Devices - Identification

- Most common forms:
  - User Name
  - User ID
  - Account Number
  - Personal Identification Number (PIN)
  - Badges
  - MAC Address
  - IP Address
  - RFID
  - Email address
  - Security Identifier (SID)
  - Relative Identifier (RID)
- User Identification Guidelines
  - Uniqueness: Must provide positive identification
  - Non-descriptive: Should not expose role or job function of the user
  - Issuance: Must be secure and documented



Identification - Security Identifier (SID) Breakdown

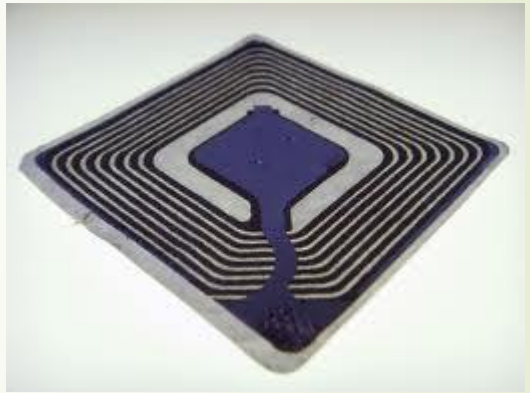
- S-1-5-21-4035617097-1094650281-2406268287-1981
  - S - identifies string as a SID
  - 1 – revision level or version
  - 5 – authority value
  - 21-4035617097-1094650281-2406268287 – local computer identifier (48 bit)
  - 1981 – Relative ID (RID) "greater than 1000 for all non-system users

Nonrepudiation

- Cannot deny an activity or event
- Established by
  - Identification
  - Authentication
  - Authorization
  - Accountability
  - Auditing

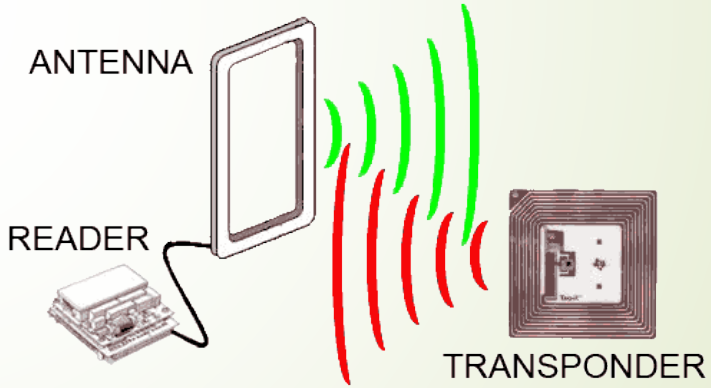
Identification & Authentication of People & Devices - Radio Frequency Identification (RFID)

- Considered to be a “dumb” device
- Three types of tags:
  - Active
  - Semi-passive
  - Passive
- Three key elements:
  - RFID tag or transponder
  - RFID tag reader or transceiver
  - Back-end database associated with the tags contents
- RF Fibers
  - Chipless tags (no integrated circuit)
  - Fiber material reflects back portion of signal
- Can be blocked by a Faraday cage or simple aluminum foil



RFID - Vulnerabilities

- Unprotected RFID tags can be vulnerable to:
  - Eavesdropping/Skimming
  - Traffic Analysis
  - Spoofing
  - DoS/DDoS Attacks
  - RFID Reader Integrity
  - Personal Privacy



Identity Management Implementation

- Set of technologies intended to offer greater efficiency in the management of a diverse user and technical environment and addresses all aspects of controlling access
- Management challenges:
  - Consistency
  - Usability
  - Reliability
  - Scalability
- Technologies include:
  - Password Management
  - Account Management
  - Profile Management
  - Directory Management
  - Single Sign On

Identity Management Implementation - Password Management

- Passwords are the most common authentication technology in use which makes password management a primary concern
- Password Management System
  - Designed to manage passwords consistently across enterprise
  - Passwords synchronized across multiple systems
  - May provide self registration procedures and personal security questions
  - At a minimum will:
    - Track password history
    - Manage password aging
    - Manage password construction and length
    - Store passwords with non-reversible encryption (hash)

Identity Management Implementation - Account Management

- One of the most risk-laden aspects of access control is the creation, modification, and decommissioning of user accounts

- Account management systems include one or more of the following:
  - Central facility
  - Workflow system
  - Automatic replication of data
  - Batch change capability
  - Automatic creation, change, or removal of access to system resources

Identity Management Implementation - Profile Management

- **Allows users to manage those parts of their profiles where data is not sensitive or require validation**
- **Done manually (administratively) or Automated (self-service)**
- **Self-Service can reduce costs and time needed to implement change**

Identity Management Implementation - Directory Management

- Provides a centralized collection of user data
- Simplifies the overall management of user data
- Improves consistency of user data as it is used between systems
- Promotes uniform security control of the environment
- Operate in a tree like structure
- Four most common directory standards:
  - X.500
  - Lightweight Directory Access Protocol (LDAP)
  - Active Directory Domain Services (ADDS)
  - X.400

Identity Management Implementation – Directory Technologies

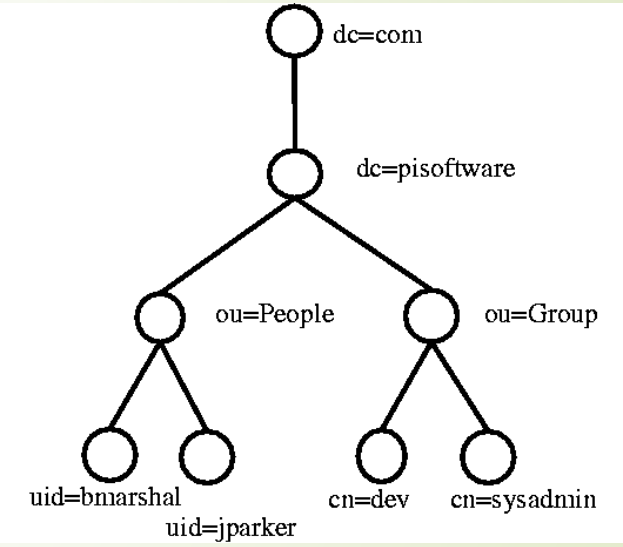
- X.500
  - ISO 9594
  - Consists of four separate protocols:
    - Directory access protocol (DAP) “primary protocol”
    - Directory system protocol (DSP)
    - Directory information shadowing protocol (DISP)
    - Directory operational bindings management protocol (DOP)

Identity Management Implementation – Directory Technologies

- Lightweight Directory Access Protocol (LDAP)
  - Based on X.500 Directory Access Protocol (DAP)
  - Provides a simpler implementation of directory services for enterprises
  - Enables you to locate organizations, individuals, files and devices in a network
  - Uses a hierarchical tree structure - Directory Information Tree (DIT)
  - Uses a client/server architecture
  - Common attributes are:
    - Distinguished Name (DN)
    - Common Name (CN)
    - Domain Component (DC)
    - Organizational Unit (OU)
  - Uses port 389 if unsecured, 636 if secured

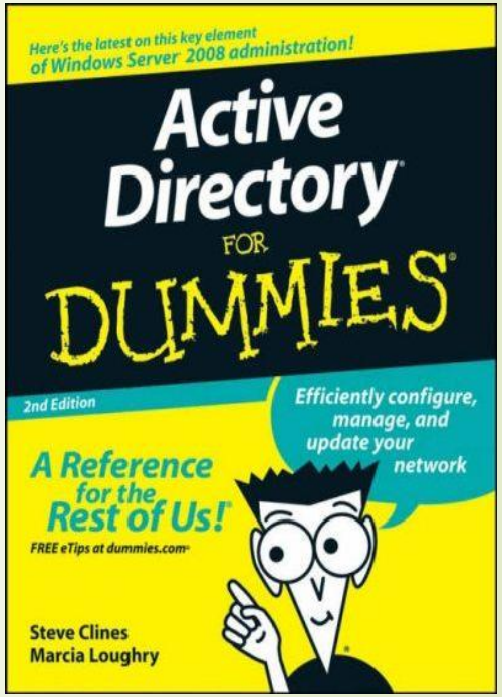
Identity Management Implementation – Directory Information Tree (DIT)

- Directory services operate in a tree like structure
  - Read from top to bottom with root at the top
  - Uses name spaces
  - Assigns distinguished names (DN)
  - Distinguished name made up of:
    - Common name (CN); domain component (DC); country code (CC); organization (O); organizational unit (OU); leaf objects (people, PCs, Printers, etc.)
    - Other descriptors are possible



Identity Management Implementation – Directory Technologies

- ADDS or Active Directory (AD)
  - Microsoft based implementation of LDAP
  - Uses LDAP for naming structure.
  - Directories are organized into forests and trees
  - Domains are identified by their DNS name
  - Objects are grouped by organizational units



Identity Management Implementation – Directory Technologies

- X.400
  - Guidelines for the exchange of e-mail
  - Known as the "Message Handling System"
  - Supports two basic functions:
    - Message transfer
    - Message storage
  - Addresses consist of a series of name/value pairs separated by semicolons
  - Largely replaced by SMTP based e-mail systems
- X.400 address specifications
  - O-organization name
  - OU-organizational unit name
  - G-given name
  - I-initials
  - S-surname
  - C-country name

Identity Management Implementation – Directory Technologies

- Single Sign-On (SSO)
  - AKA reduced sign-on or federated ID management (FIdM)
  - Provides a central repository of user credentials
  - Enables a user to log on once and access all authorized network resources
- Script-Based SSO
  - Allows an organization to develop customized scripts to implement their own solution

Identity Management Implementation – Kerberos

- Kerberos is a trusted third-party authentication protocol
- Establishes single-sign on
- Uses symmetric keys for encryption; no PKI or asymmetric encryption involved
- Four basic requirements:
  - Security
  - Reliability
  - Transparency
  - Scalability

"Guarding the gates of our Network"

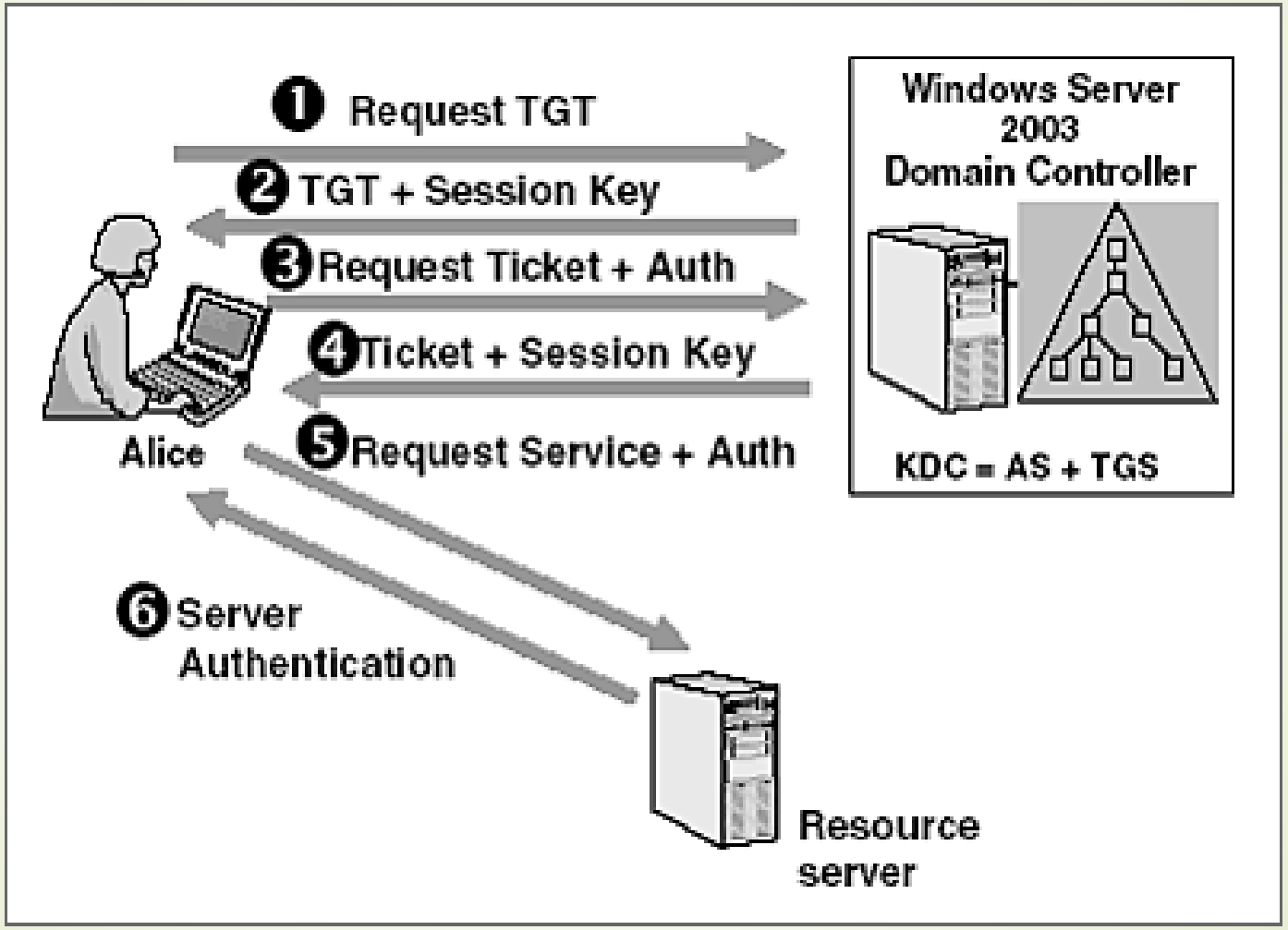
Kerberos - Elements

- Key Distribution Center (KDC)
- Authentication Server (AS)
- Ticket-Granting Server (TGS)
- Realm
- Principals
- Ticket (service ticket [ST])

Kerberos - Attributes

- Kerberos is authentication NOT authorization
- The primary goal of Kerberos is to ensure private communications between systems over a network utilizing session keys and shared secrets
- Timestamps are used in the authenticators - computer clocks must be within tolerance (5 min)
- The credentials cache is not paged and is erased upon logoff or system shut-down
- Smart Cards can be used to replace the password logon

Kerberos – Authentication Process

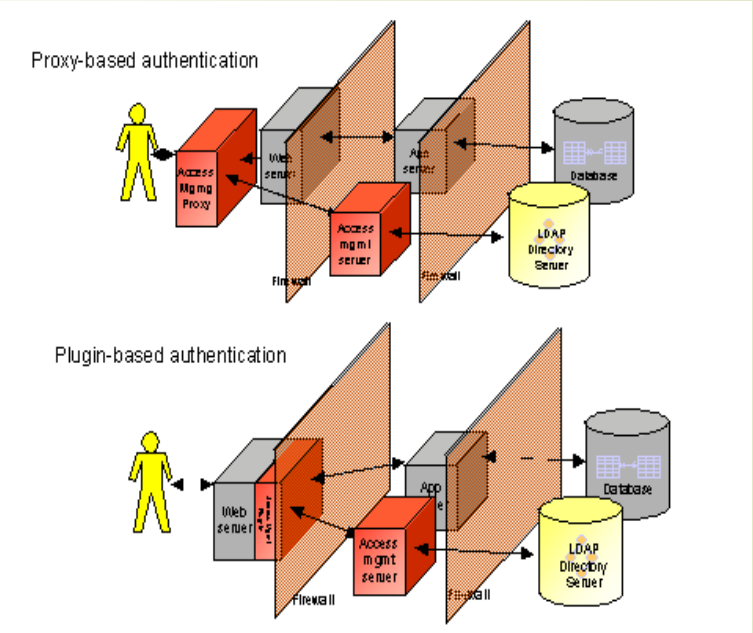


Kerberos - Weaknesses

- The KDC can be a single point of failure
- The KDC must be able to handle lots of requests in a timely manner
  - Since the KDC is a centralized key store, it must handle all requests for tickets
- Secret and Session Keys are temporarily stored on the user's workstation and could be compromised
- Authentication vulnerable to password guessing
- Network traffic is not protected by Kerberos
- User changing password, changes secret key and KDC database to update

Identity Management Implementation – Perimeter Based Web Portal Access

- **Can use LDAP directory data to manage user identity, authentication, and authorization on multiple web-based applications using web portals tied to web access management (WAM) solutions**
- **Replaces sign-on process with plug-in services managed by the WAM**
- **Provides user management and SSO**

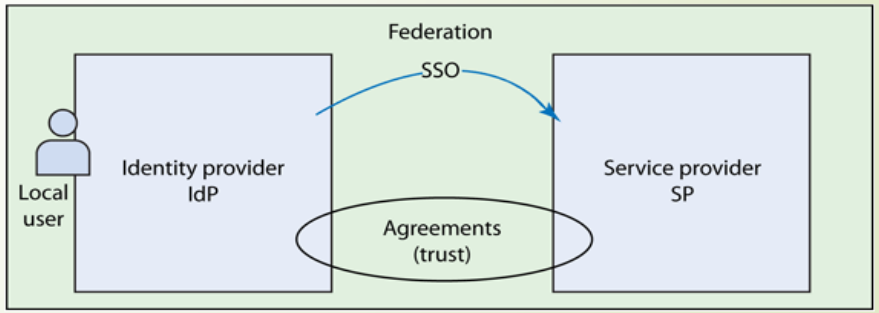


Identity Management Implementation – Federated Identity Management (FIdM)

- **When multiple organizations need to share the same applications and users between them**

- **Relies on a common set of policies, standards, and procedures for provisioning and management of user identification, authentication, and authorization information as well as a common process for access control**

- **Two basic processes:**
  - **Cross-Certification Model**
  - **Trusted 3rd Party or Bridge Model**



Identity Management Implementation – Security Assertion Markup Language (SAML)

- Used to exchange authentication and authorization data between security domains
- XML-based protocol
- Enables Web-based authentication and authorization including SSO
- Three assertion statements
  - Authentication Assertion
  - Attribute Assertion
  - Authorization Decision Assertion

SAML - Specification

- Three defined roles:
  - The principal
  - The identity provider (IdP)
  - The service provider (SP)

- Built on existing standards
  - XML
  - XML Schema
  - XML Signature
  - XML Encryption
  - HTTP
  - Simple Object Access Protocol (SOAP)

Identity Management Implementation – Once In Unlimited Access (OUIA) Model

- User authenticates once and then has access to all the resources
- System behind authentication has no authorization mechanism
- Authentication is your authorization
  - Often no certificate or token is passed between the user and the authentication system
- Unauthorized users accessing the system can have access similar to unauthorized users once access to the Intranet is obtained

Secure European System for Applications in a Multi-Vendor Environment (SESAME)

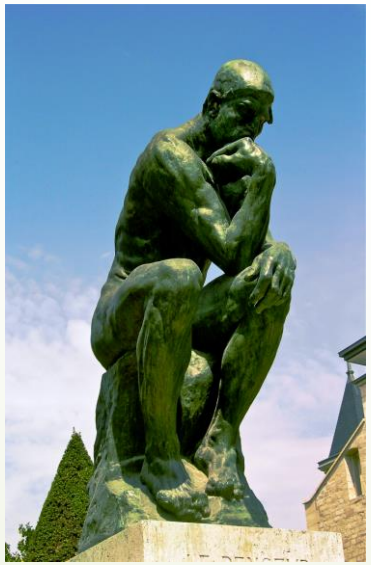
- Offers SSO
- Uses symmetric and asymmetric encryption
- Compatible with Kerberos V.5
- Uses public key cryptography to distribute secret keys
- Uses Privilege Attribute Certificates (PAC) instead of Kerberos tickets

Identity Management Implementation – Single/Multi-Factor Authentication (MFA)

- Authentication factors can be one of three types:
  - Type 1 - Something you know (knowledge)
  - Type 2 - Something you have (possession)
  - Type 3 - Something you are (characteristics)
- Single factor authentication uses one of the three types to carry out the authentication process
- Two-factor / Multi-factor Authentication (MFA) requires two (or more) different authentication types to be deployed
- Strong authentication requires two or more methods
- Mutual Authentication

Authentication Factor Type 1 – Something You Know

- PIN
- Password
- Pass phrases
- Cognitive
- Composition
- One-time

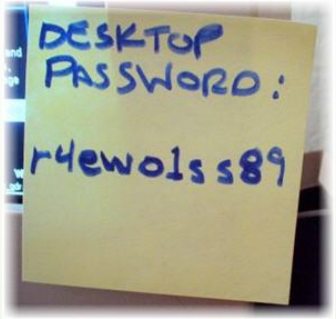


- Password Storage
  - UNIX/Linux
    - Stored as a hash
    - Stored in /etc/shadow
  - Windows
    - Stored as a hash
      - LAN Manager Hash (LM)
      - NT LAN Manager Hash (NTLM)
      - NT LAN Manager Hash Version 2 (NTLMv2)
    - Stored in the Security Account Management file (SAM)

Type 1 - Password Vulnerabilities

- Dictionary attack
- Brute force attack
- Hybrid attack
- Rainbow Tables
- Social engineering
- Key stroke loggers

- Improve security with:
  - One-way encryption
  - Account lockout
  - Auditing
  - Training
  - Salt
  - Graphical Passwords



Authentication Factor Type 2 - Something You Have

- Token Device
  - Static password token
  - Synchronous token
  - Asynchronous token
  - Challenge-Response

- Type of Token Devices
  - Memory Cards
  - Smart Cards
  - Key fob
  - Electronic Access Control (EAC)

Type 2 - Tokens

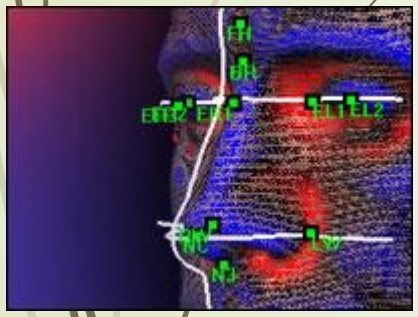
- Software or Hardware based
- The token contains a secret that is either based on asymmetric or symmetric keys
- Asymmetric key
  - Private key is stored on token
- Symmetric key
  - Shared by participants

Type 2 - Smart Cards

- Two types of smart cards
  - Contact and Contactless
- Common uses
  - Secure log on
  - Secure email/digital signatures
  - Secure web access/remote access
  - Virtual private networks (VPN)
  - Hard disk encryption
- Information contained on a smart card
  - Information that is read only
  - Information that is added only
  - Information that is updated only
  - Information with no access available

Authentication Factor Type 3 - Something You Are (Biometrics)

- Behavioral
  - Signature Dynamics
  - Keyboard Dynamics
  - Gait

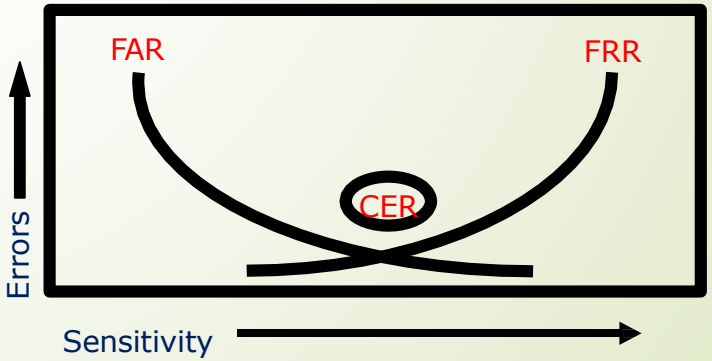


- Physiological
  - Fingerprint
  - Palm Scan
  - Hand Geometry
  - Retina Scan
  - Iris Scan
  - Facial Scan
  - Voice recognition

Type 3 - Biometric Considerations

- Resistance to counterfeiting
- Throughput and enrollment times
- Data storage requirements
- User acceptance

- Reliability and accuracy
  - Type 1 error – False Reject Rate (FRR)
  - Type 2 error – False Accept Rate (FAR)
  - Crossover Error Rate (CER)



Authentication Factor - Someplace You Are

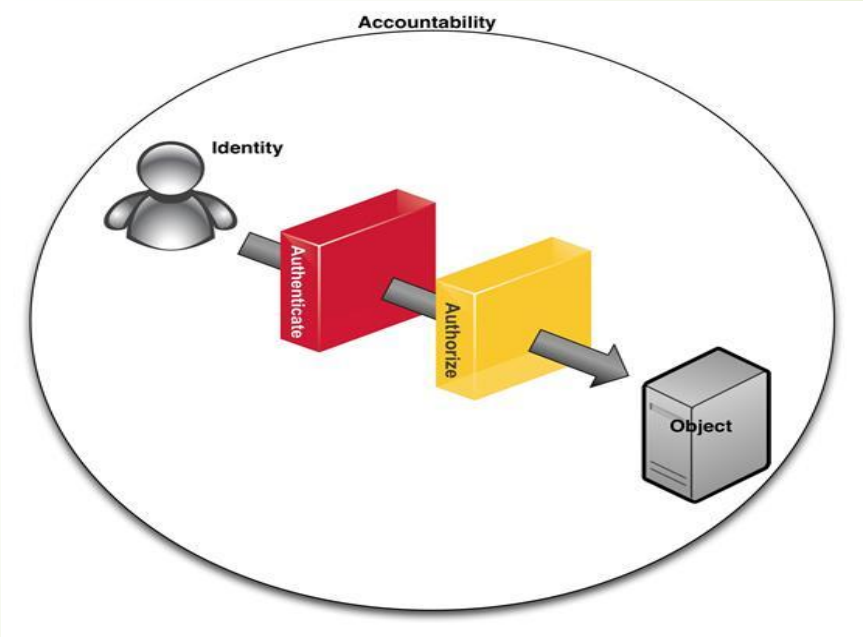
- **Location based access control**
- **Used by credit card companies to control fraud**
- **Can utilize Global Positioning Systems (GPS) or IP address based geo-location**

Authentication Types (ordered weakest to strongest)

- **Something you know (password, one time password best)**
- **Something you have on your machine (key or token stored on PC)**
- **Something you have in your possession (smart card w/pin)**
- **Something you do (keystrokes, gait, signature)**
- **Something you are (biometrics)**

Identity Management Implementation – Accountability

- Relies upon the ability to prove a subject's identity and activities
- Established by
  - Auditing
  - Authorization
  - Authentication
  - Identification



Identity Management Implementation – Accountability

- Strong Identification
- Strong Authentication
- User Training & Awareness
- Monitoring
- Audit Logs
- Independent Audits
- Policy
- Organizational Behavior

Identity Management Implementation – Auditing

- Review & examination of records and activities
- Assesses adequacy of system controls
- Ensures compliance with polices
- Detects malicious activity
- Evidence for prosecution
- Provides problem reporting and analysis

Identity Management Implementation – Session Management

- How a single instance of identification and authentication is applied to resources
  - Desktop Sessions
    - Screensavers
    - Timeouts & Automatic Logouts
    - Session/Logon Limitation
    - Schedule Limitations
  - Logical Sessions
- Provides ease of use and flexibility for the end user
- Provides an avenue of attack

Identity Management Implementation – Identity Proofing

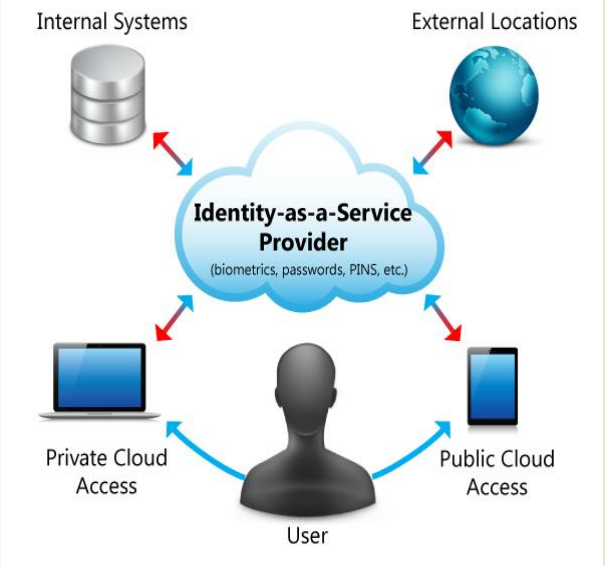
- Process of collecting and verifying information about a person for the purpose of proving that a person who has requested an account, a credential, or other special privilege is indeed who he or she claims to be
- Establishes a reliable relationship that can be trusted electronically between the individual and said credential for purpose of electronic authentication.
- Performed prior to account creation
- Implementations may include:
  - Electronic Authentication (e-authentication)
  - Personal Identity Verification (PIV)

Identity Management Implementation – Credentialing Management System

- A unified, robust, and enterprise wide user authentication and authorization framework
- Enables streamlined access without compromising the security that more sensitive applications and data demand
- Examples:
  - Windows Credentialing Management
  - Graphical Identification and Authentication (GINA) Architecture
  - General Services Administration (GSA) Credential and Identity Management System (GSAIMS)
  - GSA Access Management System (GAMS)
  - Physical Access Systems (PACS)
- Is not an enforcement mechanism

Identity as a Service (IDaaS)

- Cloud based services that broker identity and access management functions
- Combination of administration and account provisioning, authentication and authorization, and reporting functions
- Manages identity as a digital entity
- Functionality includes:
  - Identity Governance and Administration (IGA)
  - Access
  - Intelligence



IDaaS - Benefits

- Single Sign On (SSO)
- Federation
- Granular Authorization Controls
- Administration
- Integration with Internal Directory Services
- Integration with External Services

Integrate Third Party Identity Services – Cloud Computing Services

- Identity Management has been altered by the convenience of 3rd party cloud services.
- Cloud services provide on-demand service, elasticity, broad network access, reduction in expenses and total cost.
- A major shift in identity management is due to:
  - IT no longer owns the servers and applications they use
  - Provider capabilities are not fully compatible with existing internal systems
  - Users vary the ways they utilize the cloud

Cloud Computing Services - Managing Accounts

- **Managing accounts in a cloud based application and directory solution involves:**
  - **Cloud identity has no integration requirements as each user is created in the cloud and exists only in the cloud**
  - **Directory Synchronization uses existing on premises directory systems**
  - **Federated Identity can be used to implement Single Sign On**

Implement and Manage Authorization Mechanisms – Role Based Access Controls (RBAC)

- **Roles are created based on functions and tasks that a role will carry out. Users are assigned to roles, permissions are assigned to the roles and users only acquire permissions on assumption of the role**
- **Permissions assigned to a billet or position (not an individual)**
- **Ideal for high turn-over positions**

RBAC - Architecture

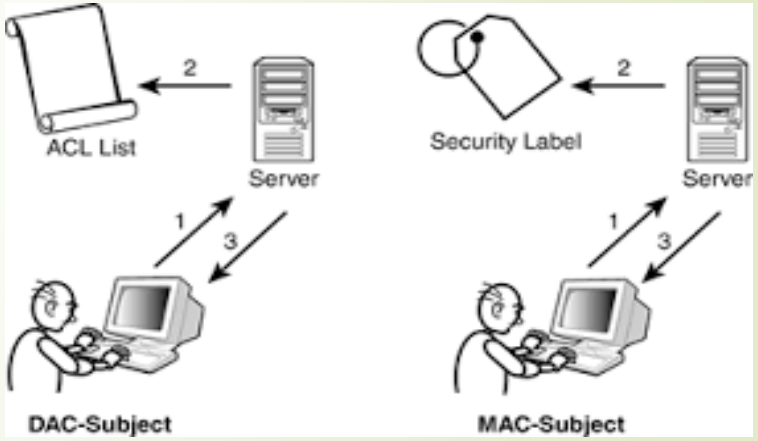
- Non-RBAC
  - User granted access to data or application with ACLs
  - No formal roles
- Limited RBAC
  - Mapped to a single role within a single application
- Hybrid RBAC
  - Role applied to multiple applications or systems
- Full RBAC
  - System is controlled by roles defined by policy and access control infrastructure and applied across the enterprise

Implement and Manage Authorization Mechanisms – Rule Based Access Control

- **Access based on predefined rules**
- **Specify privileges granted to users (read/write/execute)**
- **Applied through ACLs on routers and rules in firewalls**

Implement and Manage Authorization Mechanisms – Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

- Mandatory Access Control (MAC)
  - Based on Sensitivity Labels
  - Controlled by Security Policy Administrators
  - Users cannot over-ride Security Policy



- Discretionary Access Control (DAC)
  - Users set privileges on information they own
  - Sensitivity Labels are not required
  - Dynamic and allows the sharing of information

Additional Access Control Mechanisms

- Content-Dependent Access Control
- Context-Dependent Access Control
- Constrained (Restricted) User Interface
- Centralized Access Control
- Decentralized Access Control

Prevent or Mitigate Access Control Attacks

- Identity and Access Management (IAM) requires protection as well
- Areas where preventive and detective controls would help prevent, detect, or mitigate an attack:
  - Getting visibility and control over user access privileges
  - Detective controls designed to detect and revoke inappropriate access
  - Access policy that can prevent or detect "toxic combinations" of access privileges
  - Use automatic account reconciliation tools to detect unauthorized changes to access privileges
- Implementing the right controls can help mitigate risks and more effectively protect critical resources and customer data

Prevent or Mitigate Access Control Attacks

- Access control attacks attempt to bypass or circumvent access control methods
- Access aggregation is the process of collecting multiple pieces of non-sensitive information and combining them to learn sensitive information
  - Authorization Creep
    - User gains access rights as he/she moves around in the system or assumes new duties yet still retains past rights
  - Single Sign On
    - An intentional result moderated by Directory Services
- Reconnaissance attacks are access aggregation attacks that combine multiple tools to identify multiple elements of a system (i.e. IP address, open ports or running services)

Prevent or Mitigate Access Control Attacks

- Protecting against access control attacks requires numerous security precautions
- Proactive preventive measures include:
  - Controlling physical access to systems
  - Controlling electronic access to password files
  - Encrypting password files
  - Creating a strong password policy
  - Using password masking (i.e. display an *)
  - Actively managing accounts
  - Using vulnerability scanners
  - Deploying multifactor authentication
  - Using account lockout controls
  - Using last logon notification
  - Educating users about security
  - Auditing access controls
  - Actively managing accounts
  - Using vulnerability scanners

Identity and Access Provisioning Lifecycle

- The lifecycle is the workflow of how a user gains access, uses it, and loses it
- Lifecycle phases
  - Provisioning
    - Consider Least privilege, separation of duties, access aggregation
  - Review
    - Monitoring of access rights and usage
  - Revocation
    - Removing access temporarily (i.e. extended leave) or permanently

Questions?

Security Assessment and Testing

(Designing, Performing, and Analyzing Security Testing)

Domain Objectives

- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data
- Analyze and report test output
- Conduct or facilitate internal and third-party audits

Log Management

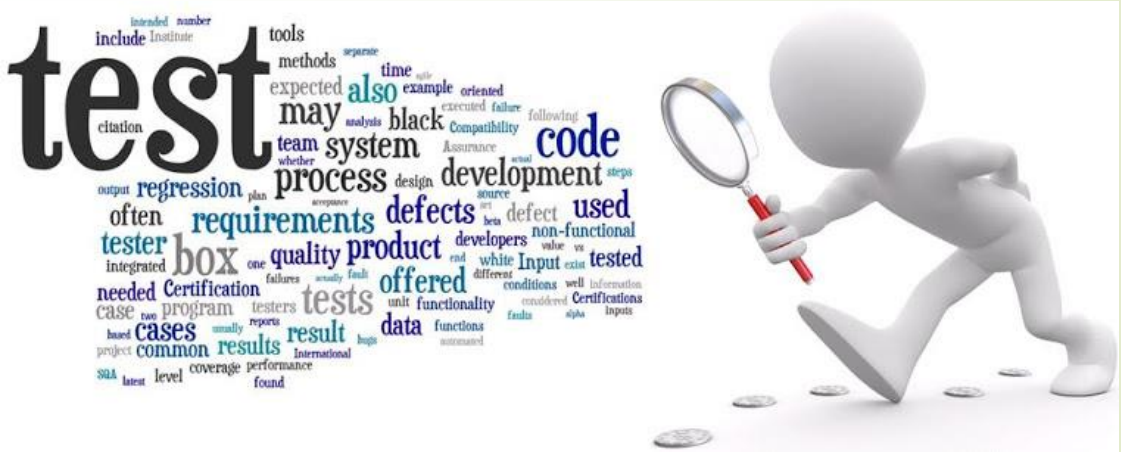
- Operational processes:
  - Configuring log sources
  - Performing log analysis
  - Initiating responses to identified events
  - Managing long-term storage
- Administrator responsibilities:
  - Monitor logging status
  - Monitor log rotation and archival
  - Check for upgrades and patches of logging software
  - Synchronizing clocks to common source
  - Reconfigure logging based on policy changes
  - Document and report anomalies
  - Ensure logs are consolidated to repositories

Synthetic Transactions

- Synthetics do not track real user sessions
  - Synthetic Performance Monitoring (proactive monitoring) follows scripted transactions that emulate those of a user
- Real User Monitoring (RUM)
  - Capturing and analyzing every transaction of every user of a website or application
  - AKA: End-User Experience monitoring (EUM)
- Bottom up RUM
  - Capturing server-side information
- Top-down RUM
  - Capturing user experience

Software Testing Methods

- Test from multiple angles
- Test from low to high
- Methods:
  - Static/Dynamic
  - White/black box
  - Traceability Matrix

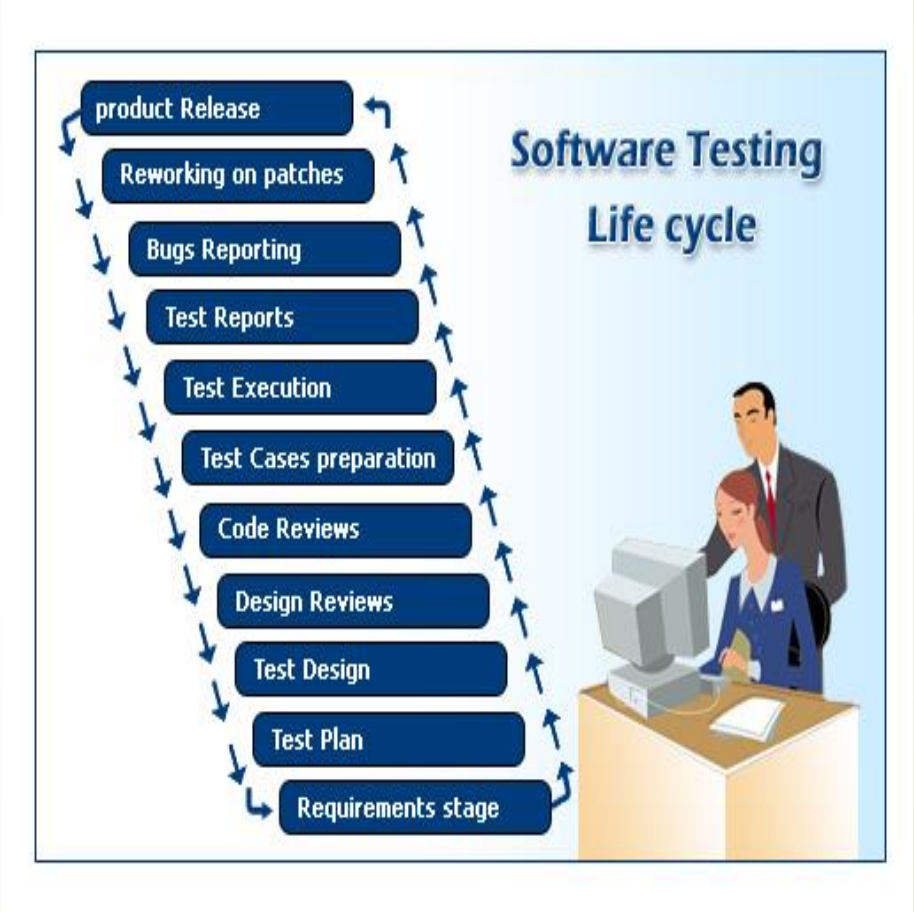


Black Box Testing

- AKA: Definition-Based Testing
- AKA: Specification-Based Testing
- AKA: Functional Testing
- Identifies test cases based on what the software/program is intended to do
- Functional testing methods:
  - Normal Case (test with expected inputs)
  - Output Forcing (Chosen test inputs produce selected outputs)
  - Robustness (correct behavior when given invalid inputs)
  - Combination of Inputs (combination of above)

Software Testing Levels

- Testing levels:
  - Interface testing
  - Alpha/Beta testing
  - Pilot testing
  - Installation testing
  - Integration testing
  - Regression testing
  - Acceptance testing
  - Function testing
  - Parallel testing
  - Sociability testing



Fuzzing

- Black box testing that uses random malformed data as input into software programs to determine if they will crash or break
- Often finds unidentified buffer overflow possibilities
- Uses software called a fuzzer
- Fuzz Testing Tools
  - Send random data to an application to attempt to crash the program

Combinatorial Software Testing

- Black box testing method
- Seeks to test all unique combinations of software inputs
- Example: pairwise testing
  - 8 steps could be tested in 4 steps by pairing up requirements.

Testing During Application Development

- When the application is not mature enough to place it in the test environment
- Static Source Code Analysis (SAST) and Manual Code Review
  - Analyze source code without executing the application
  - Examine source code for insecure programming, outdated libraries, and misconfigurations
- Static Binary Code Analysis and Manual Binary Review
  - Analysis of the binary code (compiled program), looking for vulnerabilities without executing the program

Testing During Application Development

- Methods when the software can be executed
- Manual or Automated Penetration Testing
  - Simulate the activity of an attacker
- Automated Vulnerability Scanners
  - Detect for well known vulnerabilities

Software Testing Tenets

- Expected test outcome is predefined
- Good testing has a high probability of finding an error
- Successful testing finds errors
- Testing is independent from coding
- Employ both user and programmer expertise
- Use different programs than those of the programmer
- Test documentation is reusable
- Examining only the usual case is insufficient

White Box Testing

- AKA: Structural Testing
- AKA: Code-Based Testing
- Identifies test cases from examining the source code
- Structural testing can identify "Dead Code"
  - Code that is never executed during program execution
- Testing can be extended by using metrics to show the percentage of software structure that has been evaluated.
- Metrics are usually referred to as "coverage". This usually means 100% coverage of the software. Each program piece has been executed at least once.

Common Structural Coverage Metrics

- Statement Coverage
- Decision Coverage
- Condition Coverage
- Multi-Condition Coverage
- Loop Coverage
- Path Coverage
- Data Flow Coverage

Software Maintenance Tasks

- Software Validation Plan Revision
- Anomaly Evaluation
- Problem Identification and Resolution Tracking
- Proposed Change Assessment
- Task Iteration
- Documentation updating

Testing Strategies

- Good practice to combine methods to achieve the greatest test coverage
  - Positive Testing
    - Determines an application functions as expected
    - If an error is encountered, the test fails
  - Negative Testing/Misuse Case Testing
    - Ensures an application can properly handle invalid input or unexpected user activity
    - Exceptions are expected

Typical Negative Testing Scenarios

- **Populating Required Fields (leave empty)**
- **Correspondence between Data and Field Types (enter incorrect data types)**
- **Allowed Numbers or Characters (too many/too few)**
- **Allowed Data Bounds and Limits (exceed range)**
- **Reasonable Data (invalid data)**
- **Web Session Testing (open web pages without logging in)**

Information Security Continuous Monitoring (ISCM)

- **Maintaining ongoing awareness of information security, vulnerabilities, and threats**
- **Supports risk management decisions**
- **Strategy based on risk tolerance**
- **Analyze data collected, report findings and determine response.**
- **Respond to findings with mitigating, acceptance, transference or avoidance activities.**
- **Review and update the monitoring program, adjusting strategy accordingly**

Information Security Continuous Monitoring (ISCM) Strategy

- **Encompasses technology, processes, procedures, operating environment, and people**
- **Strategy:**
  - **Understands risk tolerance and helps set priorities and manage risk**
  - **Includes metrics to indicate security status**
  - **Verifies compliance with security requirements**
  - **Maintains visibility of asset security**
  - **Ensures knowledge of change control**
  - **Maintains awareness of threats and vulnerabilities**

Reporting

- Any data collected that is not required for reporting purposes or found to not be useful in maintaining or improving an organization's security posture:
  - Should be evaluated to be discontinued to save resources
  - Factors that can change monitoring strategy:
    - Change to core mission
    - Change in enterprise architecture
    - Change to risk tolerance
    - Change in threat information
    - Change in vulnerability information
    - Change within information systems
    - Trend analysis
    - New laws or regulations
    - Change in reporting requirements

Internal and Third Party Audits

- Federal agencies are subject to Federal Information Security Management Act (FISMA) requirements
- FISMA requires agencies to self-audit with an independent audit review annually
- Statement on Auditing Standards (SAS) reports are used to gain comfort over outsourced activities
  - SAS focus is on internal control over financial reporting and not availability or security
- Service Organizational Control Reports replace SAS reports to cover the assurance needs

Service Organizational Control (SOC) Reports

- 3 types of reports
- Period of time reports (covering design and operational effectiveness) are type 2
- Point in time reports are type 1
- Type 3 is referred to as a SysTrust, WebTrust, or Trust Service report

Service Organizational Control (SOC) 1

- **Focuses on financial reporting risks and controls specified by the service provider**
- **Especially important when service provider performs financial transaction processing or supports transaction processing systems**

Service Organizational Control (SOC) 2/ 3

- **Focus on:**
  - **Security**
  - **Availability**
  - **Confidentiality**
  - **Processing integrity**
  - **Privacy**

Examples of Security Topics

- IT security policy
- Security awareness
- Risk assessment
- Physical access
- Security monitoring
- Incident management
- Asset classification
- Personnel security
- Configuration management
- Change management
- Monitoring and compliance

Examples of Availability Topics

- **Availability policy**
- **Backup and restoration**
- **Environmental controls**
- **Disaster recovery**
- **Business continuity management**

Examples of Confidentiality Topics

- **Confidentiality policy**
- **Confidentiality of inputs**
- **Confidentiality of data processing**
- **Confidentiality of outputs**
- **Information disclosures (including 3rd parties)**
- **Confidentiality of information in systems development**

Processing Integrity Topics

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs
- Information tracing from source to disposition

Privacy Topics

- Management
- Notice
- Choice and consent
- Collection
- Use and retention
- Access
- Disclosure to third parties
- Quality
- Monitoring and enforcement

First Time Audits

- **Audit Preparation Phase**
  - **Define audit scope and timeline**
  - **Identify existing or required controls**
  - **Perform readiness review to identify gaps**
  - **Communicate prioritized recommendations**
  - **Discuss alternative and remediation plans**
  - **Verify gaps have been closed**
  - **Determine the most effective audit and reporting approach**

First Time Audits

- **Audit Phase**
  - **Provide overall project plan**
  - **Complete advance data collection**
  - **Conduct on-site meetings and testing**
  - **Complete off-site analysis of collected information**
  - **Conduct weekly reporting of status and issues**
  - **Provide a draft report for managerial review**
  - **Provide an internal report for management with overall observations and recommendations for consideration**

Audit Trail Monitoring

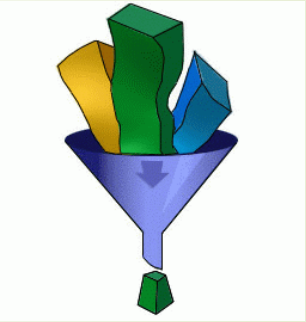
- Log Sources
  - Network: Antivirus, IDS/IPS, VPN, Web, Vulnerability Management, Authentication Servers, Routers, and Firewalls
  - Operating Systems: System and Audit records
  - Applications: Client/Server responses and requests, Usage, Significant Operational Actions
- Audit Event Types:
  - Network
  - System
  - Application
  - User
  - Keystroke Monitoring

Monitoring

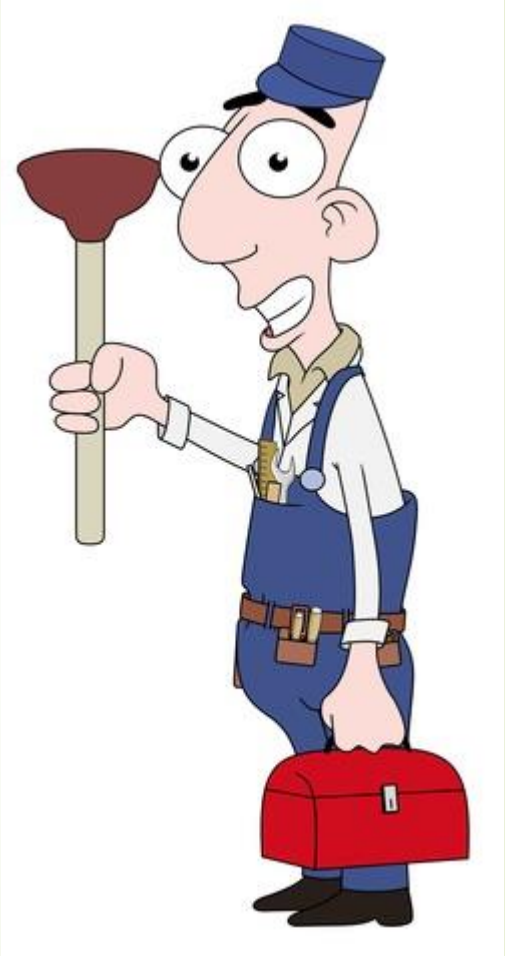
- Reasons for monitoring
  - Logging events
  - Reviewing events

Auditing Issues and Concerns

- Following are best practices in addressing audit issues and concerns:
  - Control the volume of data (don't allow rollover logs)
  - Event filtering of clipping level determines the amount of log details captured
  - Audit tools can reduce log size
  - Establish procedures in advance
  - Train personnel in pertinent log review
  - Protect and ensure against unauthorized access
  - Disable auditing or deleting/clearing logs
  - Protect the audit logs from unauthorized changes
  - Store/archive audit logs securely



Questions?



Security Operations

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

Domain Objectives

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Conduct incident response
- Operate and maintain preventive measures
- Implement and support patch and vulnerability management

Domain Objectives con't

- Participate in and understand change management processes (versioning, baselining, security impact analysis)
- Implement recovery strategies
- Implement disaster recovery processes
- Test disaster recovery plans
- Participate in business continuity planning and exercising
- Implement and manage physical security
- Participate in personnel safety (duress, travel and monitoring)

Physical (Environmental) Security Challenges

- Threats and Vulnerabilities
  - Threat Types
    - Natural and Environmental Threats
    - Supply System Threats
    - Manmade Threats
      - Malicious Threats
      - Accidental Threats
    - Politically Motivated Threats
  - Vulnerabilities
    - Inadequate or lapsed security working practices

Investigations - Digital Forensic Science

- Encompasses all domains in which the evidence or potential evidence exists in a digital or electronic form whether in storage or on the wire and includes:
  - Computer Forensics
  - Digital Forensics
  - Network Forensics
  - Electronic Data Discovery
  - Cyber Forensics
  - Forensic Computing

- The Digital Forensic Science Research Workshop defines it as:
  - The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations

Investigations - Crime Scene

- Digital crime scenes are physical (i.e. server) and virtual (i.e. data on a Storage Area Network [SAN])
- Identify the scene
- Protect the environment
- Identify evidence and potential sources of evidence
- Collect evidence
- Minimize the degree of contamination
- Start the Chain of Custody

Investigations - Crime Scene

- Understanding the following will help correctly identify the root cause of an incident:
  - Locard's Exchange Principle states that a perpetrator will:
    - Leave something behind
    - Take something with them (Evidence Dynamics)
      - exchange principle

  - M.O.M. - Behavior of suspects:
    - Motives – who and why
    - Opportunity – where and when
    - Means – capabilities a criminal would need to be successful
  - Modus Operandi (MO) – the way a crime was committed

Investigations – General Guidelines

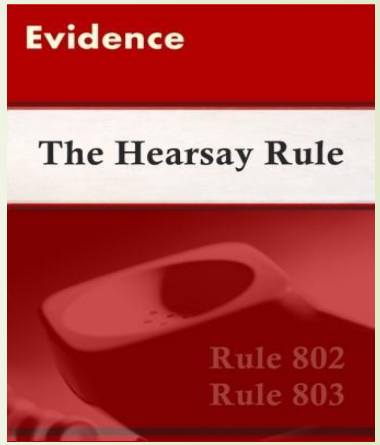
- International Organization on Computer Evidence (IOCE) devised guidelines for computer forensics and digital/electronic evidence:
  - All of the general forensic and procedural principles must be applied
  - Actions taken should not change evidence
  - Person investigating should be trained for the purpose
  - All activity must be fully documented, preserved and available for review
  - An individual is responsible for all actions taken with respect to digital evidence
  - Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles

Investigations – General Guidelines

- Investigation methodology
  - Minimize handling/corruption of original data
  - Account for any changes and keep detailed logs of your actions
  - Comply with the five rules of evidence
  - Do not exceed one's knowledge
  - Follow your local security program policy and obtain written permission
  - Capture as accurate an image of the system as possible
  - Be prepared to testify
  - Ensure your actions are repeatable
  - Collect evidence quickly and accurately
  - Proceed from volatile to persistent evidence
  - Do not run any programs on the affected system

Types of Evidence

- Real (or Physical)
- Documentary (Hearsay Rule)
- Best
- Secondary
- Direct
- Conclusive
- Circumstantial
- Corroborative
- Opinion
- Hearsay
- Exculpatory



Investigations – Policies, Roles and Responsibilities

- Corporate incident handling and response policy
  - Articulated procedures and guidelines that consider legal requirements
  - Management and handling of evidence
- Staff can be virtual (additional duty) or permanent
- Core areas to represent on response team
  - Legal, human resources, communications, executive management, physical security, internal audit, IS security and IT
  - Business units and various system administrators

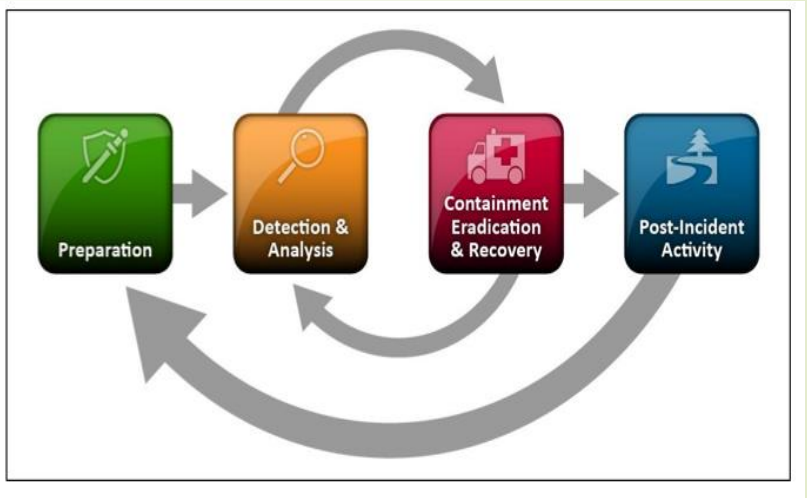
Investigations – Incident Response

- Develop a response capability
- Incident Handling and Response
  - Triage Phase (detect, identify, notify)
  - Investigative Phase (collect relevant data)
  - Containment Phase
  - Analysis and Tracking Phase
    - Root Cause Analysis
- Recovery Phase
  - Recovery, repair and prevention
- Debriefing/Feedback

NIST Incident Handling Guide

- Incident Response steps:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post Incident Activity

- Standard Six Step Model
  - Preparation
  - Detection and Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned



Types of Attacks Requiring Incident Response

- Threat Agents
- Threat Vectors
- Password Guessing and Cracking
- Session Hijacking and MITM
- Malware
- DoS/DDoS

Incident Response - Root Cause Analysis (RCA)

- Focuses on determining the root cause of an incident
- Goes deeper than identifying only the symptoms
- Burrowing down through a problem until a single cause is evident
- Determine the history of an event and work backwards to ascertain the cause
- RCA can cross boundaries between the technical, administrative and cultural areas
- Senior management must support the analysis to be successful

Investigations – Evidence Collection and Handling

- Chain of Custody (COC) refers to the who, what, when, where, and how the evidence was handled from its identification through its entire lifecycle

Hard Drive/Computer Details

Description:		
Manufacturer:	Model #:	Serial #:

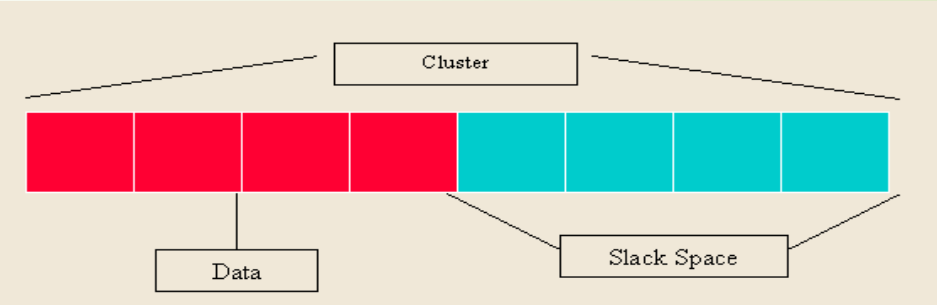
Chain of Custody

Date/Time:	From:	To:	Reason:
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	

Investigations – Understanding Forensic Procedures

- Five (5) Rules of Digital Evidence:
  - Authentic
  - Accurate (Reliable)
  - Complete
  - Convincing (Believable)
  - Admissible (Fragile)
    - Must meet 3 Requirements to be Admissible:
      - Relevant
      - Material
      - Competent

Investigations – Understanding Forensic Procedures



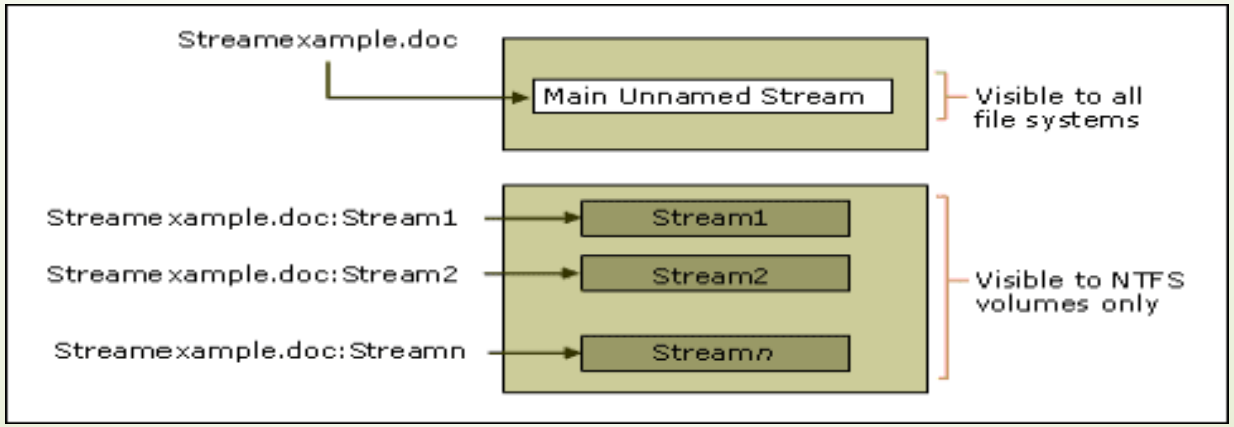
- Digital/Electronic evidence is very fragile
  - Collect very quickly and in order of volatility

- Media Analysis
  - Involves the recovery of information/evidence from information media such as hard drives, DVDs, CD-ROMs or portable memory devices.
- Network Analysis
  - Analysis and examination of data from network logs and network activity for use as potential evidence
- Software Analysis
  - The analysis and examination of program code

- Hardware/Embedded Device Analysis
  - Analysis of mobile devices

Alternate Data Streams (ADS)

- NTFS allows files to be associated with more than one data stream
- One file can be a link to multiple Alternate Data Streams of files of any size
- Difficult to detect: Doesn't show up when you run c:\dir



Investigations – Role of the First Responder Guidelines

- The first responder is the first person who arrives to investigate and respond to any detected activity
- This includes, but is not limited to:
  - System administrators
  - Computer Network Defense Service Provider (CNDSP) technical staff
  - Counter Intelligence (CI)
  - Law Enforcement (LE)

Your Security has Been Breached

- Be Aware
  - A first responder will often respond to a system still under attack
  - Be prepared to assess an active attack
  - Be prepared to treat the computer system as a crime scene
  - Respond already knowing your course of action per the given situation

Reasonable Searches

- 4th Amendment protects American citizens from unreasonable searches and seizure

- Types of searches:
  - Consent,
  - Plainview (plainview doctrine),
  - Search incident to arrest (plainview)
  - Protective sweep search (plainview)
  - Search warrant
  - Writ of possession; take charge of evidence if it is in danger of being destroyed.
  - EXIGENT CIRCUMSTANCE=judge decides admissibility if evidence obtained prior to search warrant.

Types of Responses to Incidents

- Hands Off
  - May need to wait for a trained analyst to properly collect evidence
- Shutdown
  - Determine if shutting down the computer is necessary
- Live
  - Memory contains evidence that does not survive reboot
- Postmortem vs. Live Investigations
  - The situation will dictate which method is best to use while causing the least impact

Investigations – Information, Instrumentation and Interviewing

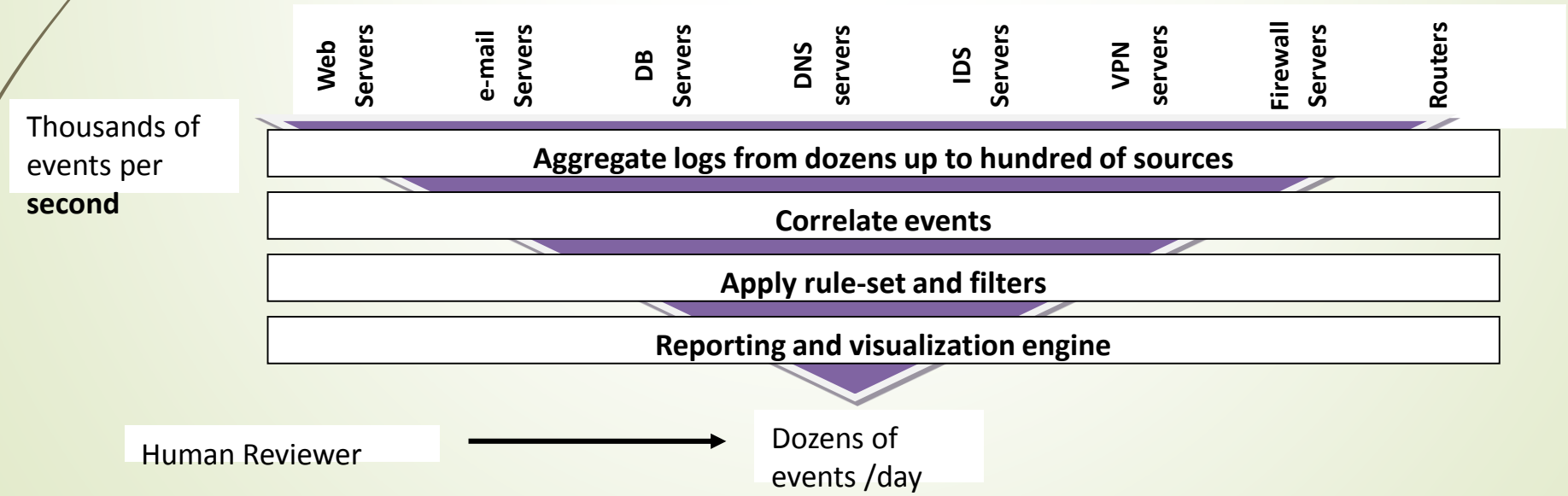
- Three components of a criminal investigation:
  - Information
    - Information accumulation (most important)
  - Instrumentation
    - Method to gather information
  - Interviewing
    - Method to gather information

Investigations - Evidence Collection and Processing

- Intrusion Detection and Prevention Systems
  - Electrical Circuit
  - Light Beam
  - Different Types of Energy Fields
    - Passive Infrared Sensors (PIR or PID)
      - Measures light energy level
      - Detects heat and movement
    - Microwave and Ultrasonic Systems (invisible)
    - Electro-static
- Sounds and Vibration
- Motion
- Coaxial Strain-Sensitive Cable
- Time Domain Reflectometry (TDR) Systems
- Balanced Magnetic Switch (BMS)

Investigations – Evidence Collection and Processing

- Security Event Management (SEM) / Security Incident and Event Management (SIEM) aggregates log information
  - Store raw information from various system logs
  - Aggregate the information in a single repository



Investigations – Continuous and Egress Monitoring

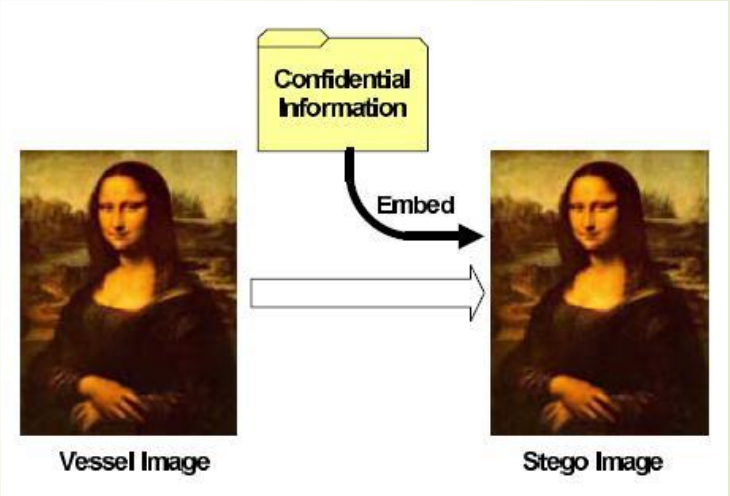
- Continuous Monitoring as a Service (CMaaS)
  - Driven by a focus on Cyber Defense
  - Supported by the Continuous Diagnostics and Mitigation (CDM) Program
    - Provides specialized IT tools and CMaaS to combat cyber threats in the civilian ".gov" networks
  - Cloud service providers exist to support an enterprise architecture
- Egress Monitoring
  - Is the monitoring and potentially restricting the flow of information that is outbound
  - Egress filtering ensures that unauthorized or malicious traffic does not leave the network

Investigations – Continuous and Egress Monitoring

- Data Leak/Loss Prevention (DLP)
  - Technologies aimed at stemming the loss of sensitive information
  - Focuses on location, classification, and monitoring information in transit, storage, or being processed
  - 3 key objectives
    - Locate and catalog sensitive information (storage)
    - Monitor and control the movement of sensitive information (transit)
    - Monitor and control the movement of sensitive information on the system (processing)

Investigations – Steganography and Watermarks

- Greek steganos, hidden or covered, plus graphein, to write
- Buries a message by taking the least significant bit of every byte to carry the secret message
- Hides a message within another medium:
  - Graphics, Sound files, etc.
- Watermarks
  - Prove ownership



Provisioning of Resources through Configuration Management

- Configuration Management (CM) is the discipline for evaluating, coordinating, approving or disapproving, and implementing changes in artifacts that are used to construct/maintain software systems
- Purpose is to establish and maintain the integrity of the product/system/item being managed throughout its lifecycle
- The CM policy should define:
  - The set of artifacts under the jurisdiction of the CM
  - How artifacts are named
  - How artifacts enter/leave the controlled set
  - How the artifact is allowed to change
  - How different versions of artifacts are made available
  - How CM tools are used to enable/enforce CM

Configuration Management – Capability Maturity Model Integration (CMMI)

- Developed to integrate software and systems engineering
- Made up of 6 Process Maturity Levels
  - Level 0 Nonexistent: processes are not performed
  - Level 1 Initial: recognize issues – no plan of action
  - Level 2 Repeatable – developed security processes
  - Level 3 Defined – security processes standardized
  - Level 4 Managed – enterprise wide security integration
  - Level 5 Optimizing – world class level of security, continuous improvement

Functional Security Operations Concepts – Key Themes

- Maintain Operational Resilience
  - Maintaining the expected levels of service availability and integrity
- Protecting Valuable Assets
  - Protect sensitive of critical resources from compromise
- Controlling System Accounts
  - Provide checks and balances against privileged accounts
- Managing Security Services Effectively
  - Reporting and continuous service improvement practices

Functional Security Operations Concepts – Controlling Privileged Accounts

- Users that require some level of special access or special privileges in order to perform a given task
- Management of Privileged Entities is very important due to the fact that these entities often have the ability to bypass security controls

Controlling Privileged Accounts - Privileged Accounts

- System Administrators
  - Ensure that a system or systems functions properly for users
  - Perform maintenance and monitoring tasks
  - Require the ability to affect critical operations such as boot sequence, log files, and passwords
  - Manage hardware and software for workstations and servers

Controlling Privileged Accounts - Privileged Accounts

- Operators
  - Have elevated privileged, but less than administrators
  - Can usually perform the following:
    - Start the operating system
    - Monitor process execution
    - Mount / Dismount volumes
    - Control jobs
    - Bypass / Rename labels

Controlling Privileged Accounts - Privileged Accounts

- Security Administrators
  - Provide oversight for the security operations of a system
  - Usually have fewer rights than system administrators
  - Ensure separation of duties is enforced
  - Provide a check and balance of power to system administrators
  - Ensure security policies are enforced

Controlling Privileged Accounts - Privileged Accounts

- Ordinary Users
  - Only have access to applications and systems necessary for them to perform a given task
  - Should not be able to monitor processes
  - Must operate within security labels
  - Should be prevented from altering the boot process

Controlling Privileged Accounts - Privileged Accounts

- Service Account
  - Dedicated to providing a system service
  - Usually run background services/daemons
  - Often assigned elevated privileges upon install of an operating system
  - Many are created by database installations

Functional Security Operations Concepts – Monitoring Special Privileges

- Those with the most access require the most watching
- Job functions that require greater scrutiny:
  - Account creation/modification/deletion
  - System reboots
  - Data backup
  - Data restoration
  - Source code access
  - Audit log access
  - Security configuration capabilities

Functional Security Operations Concepts – Service Level Agreements (SLAs)

- Is a contract between vendor and customer determining service expectations
- Attestation (3rd party audit or review)
- Right to Pentest/Right to Audit
- Secure Procurement
- Vendor Governance
  - Ensuring that vendors provide the expected value

Resource Protection

- Tangible assets
  - Physical in nature
    - Traditional property
- Intangible assets
  - Not physical in nature
    - Intellectual property

Resource Protection - Media Management

- Information resides on various media types
- Media may be a soft or hard copy
- Media containing sensitive or confidential information should be encrypted
- Removable media present different security risks
- Media should be destroyed or properly disposed

Resource Protection - Media Management

- Archival and Offline Storage
  - Requires appropriate and suitable technical solutions be in place and that there are procedures in place to ensure that recovery can be done quickly and effectively
  - Backups and archives are two methods used to store information
    - May need to migrate to new media on a regular basis
    - Requires regular testing
- Cloud Storage
  - A data storage model where the digital data is stored in logical pools
- Virtual Storage
  - Is the pooling of physical storage from multiple network storage devices

Drive/Tape Encryption

- Encryption is recommended for all portable media and devices. It can also be used for data that is static (stationary)
- Whole disk encryption
  - Recommended for mobile devices
  - Partial encryption may not protect temporary files or unallocated space from access
- Personally Identifiable Information (PII)
  - Many breach laws contain exclusions for data that has been encrypted

Resource Protection - Problem Management

- Principles of Problem Management:
  - Prevent problems and resulting incidents from occurring
  - Eliminate reoccurring incidents
  - Minimize impact of incidents
- Conflicts between problem management and incident management:
  - Incident management is concerned with restoring service as quickly as possible
  - Problem management is concerned with determining and eliminating the cause
- Critical Success Factors (CSF)
  - Avoid repeat incidents
  - Minimize impact

Preventative Measures Against Attack

- Guard against Unauthorized disclosure
- Prevent destruction, interruption, and theft
- Prevent corruption and improper modification

Preventative Measures Against Attack – Network Intrusion Detection System (NIDS) Architecture

- Incorporated into the network in a passive architecture (i.e. minimum impact to the network)
- Analyzes the contents of every packet
- May be active or passive in nature
- Does not inspect encrypted packets
- Host-Based Intrusion Detection (HIDS) is the implementation of IDS capabilities on a host level)

IDS - Analysis Engine Methods

- Stateful Matching Intrusion Detection
  - Overall behavior rather than individual packets
- Statistical Anomaly-Based Intrusion Detection
  - Patterns that deviate from the predicted norm
- Protocol Anomaly-Based Intrusion Detection
  - Deviation from expected behavior of known protocols
- Traffic Anomaly-Based Intrusion Detection
  - Deviation from expected behavior based on traffic structure

IDS - Alarms and Signals

- Meant to notify people and systems of adverse events
- Three fundamental components
  - Sensor
    - Detection mechanism
  - Control and Communication
    - Handling the alert information
  - Enunciator
    - Relay system

Preventative Measures Against Attack – Whitelisting, Blacklisting, Greylisting

- Whitelist
  - Known good
- Blacklist
  - Known bad
- Greylist
  - Not fully trusted

Preventative Measures Against Attack – Third-Party

- Sandboxing - lets programs and processes run in their own isolated virtual environment
- Anti-Malware - tools used for malware and virus mitigation
- Honeypot - decoy servers/systems set up to gather information about an attacker/intruder
  - Entrapment
  - Enticement
- Honeynet - two or more honeypots on a network and is used for monitoring a larger and more diverse network
- Honeyfarm - a centralized collection of honeypots and analysis tools

Preventative Measures Against Attack – Anti-Malware Testing Standards Organization (AMTSO)

- Four areas of focus
  - Discussion forum on testing of anti-malware
  - Developing and publicizing standards and best practices
  - Promoting anti-malware education and awareness
  - Providing tools and resources to aid standard based testing
- Support two "Feature Settings Check" webpages that allow one to test their anti-malware solutions
  - Windows
  - Android

Patch and Vulnerability Management

- Formalize procedures through change and configuration management
- Objective is to create a consistently configured environment that is secure against known vulnerabilities in OSs and application SW
- Patch testing should address proper functionality of the system and the overall effect the patch has on the state of security or policy of the system
- Key component is the intake and vetting of information regarding both security issues and patch release

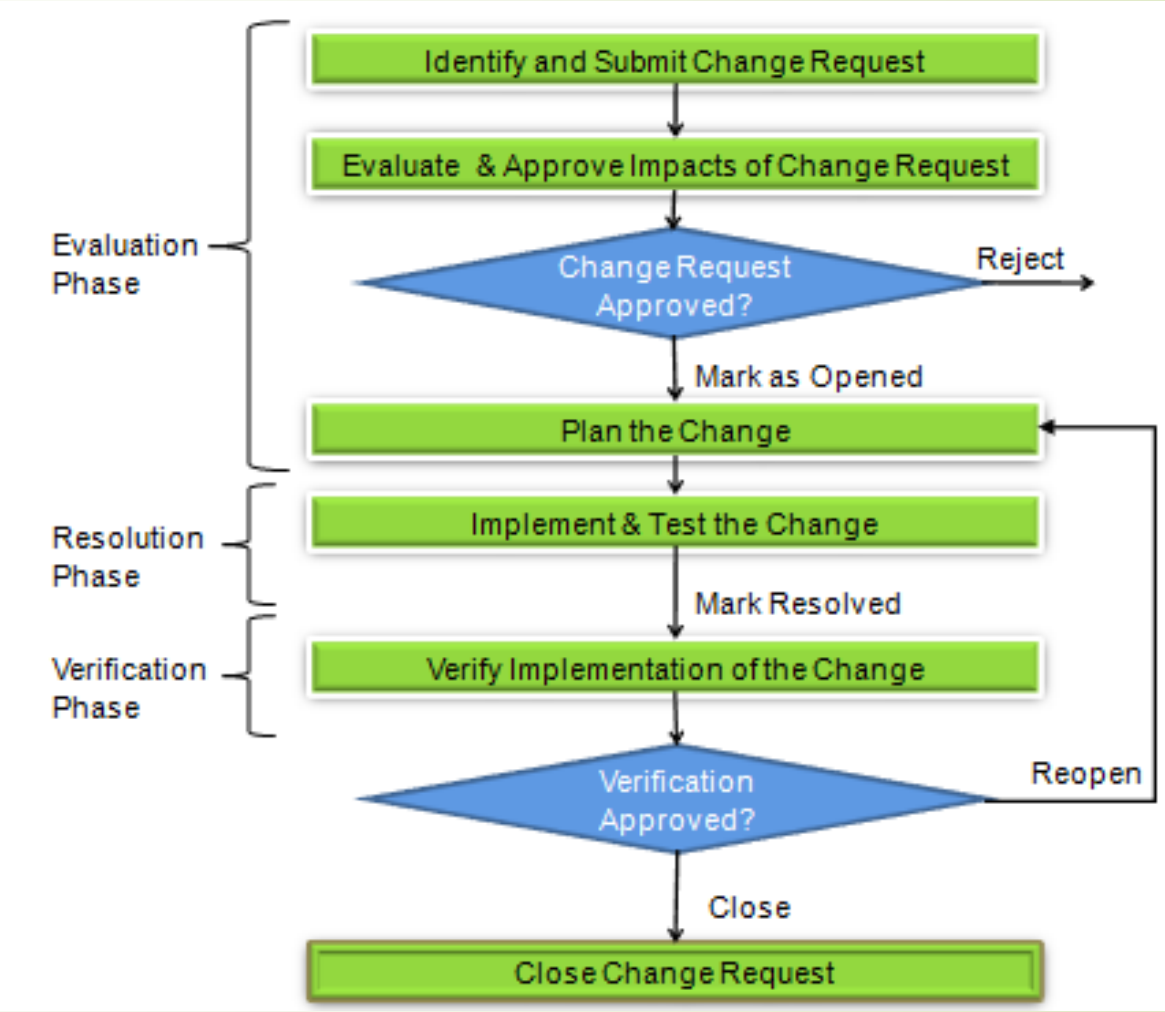
Change and Configuration Management

- Change Control Management is the process of maintaining system integrity
  - Requests
  - Impact Assessment
  - Approval/Disapproval
  - Notification
  - Implementation
  - Validation
  - Documentation

- Configuration Management is a process for identifying and documenting HW components, SW, and the associative settings which ensures that resources are properly deployed and managed
  - Requires a detailed inventory of HW and SW

Change Control Process

- Changes are always controlled
- Formalized testing process
- Ability to reverse changes
- Users informed of impending changes
- Change effects are analyzed
- Minimizes negative impact of changes



Configuration (Change) Control Board (CCB)

- Typically oversees and coordinates the change control process
- Gathers and documents sufficient details to understand the change
- The decision to implement the change and the timeliness will be driven by principles of risk and cost management
- Business continuity planners should be members of the board to assess the changes effect on recovery procedures

Change and Configuration Management – Develop a Recovery Strategy

- Surviving site
- Self-service
- Internal arrangement
- Reciprocal/Mutual Aid Agreements
- Dedicated alternate sites
- Work from home
- External suppliers
- No arrangement

Change and Configuration Management – Recovery Site Strategies

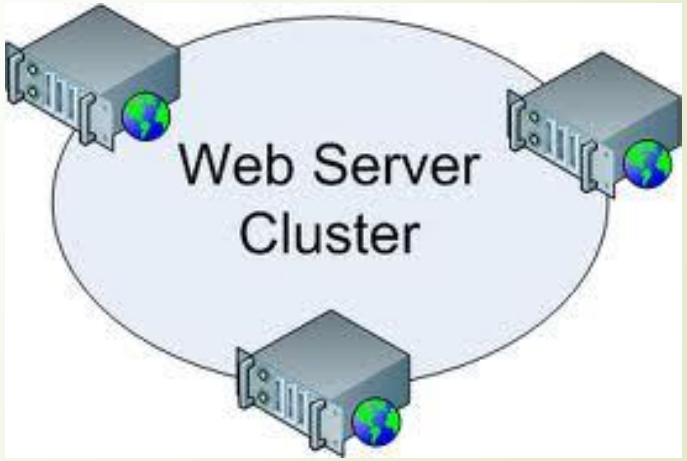
- Dual data center (most expensive, no recovery needed)
- Internal hot site (expensive, allows for testing)
- External hot site (expensive, operational within hours)
- Warm site (less expensive, not testable)
- Cold site (less expensive, not testable)
- Mobile Sites
- Processing Agreement
- Outsourcing
- Service Level Agreement (SLA)
- Multiple Processing Sites

Change and Configuration Management – System Resilience and Fault Tolerance Requirements

- Maintain the security and reliability of key computing systems to ensure it is:
  - Resilient
  - Capable of reacting automatically to common failures and address the problem without human intervention
- Trusted paths provide trustworthy interfaces into privileged user functions
  - Intended to ensure that communication paths cannot be intercepted and includes:
    - Fail-Safe – mechanisms focus on failing with a minimum of harm to personnel or system
    - Fail Secure – focuses on failing in a controlled manner to block access while the system is in an inconsistent state

System Resilience and Fault Tolerance Requirements – Redundancy and Fault Tolerance

- Involves using redundant servers or networks and redundant data storage
- Spares are components that are available if a primary component is damaged or unavailable
  - Cold spare
  - Warm spares
  - Hot spares
- High Availability Clusters (failover clusters)
  - Active-Active
    - Load balancing (hot spare)
  - Active-Passive
    - Hot standby (warm spare)
    - Located in storage (cold spare)



Redundancy and Fault Tolerance – Drives and Data Storage

- Storage Area Network (SAN)
  - Operates at block level
  - Dedicated storage on a dedicated network
- Network Attached Storage (NAS)
  - Operates at the file level
  - Typically on a shared network and can be mapped as network drives

Drives and Data Storage – Redundant Array of Independent Disk (RAID) Levels

- RAID 0
- RAID 1
- RAID 2
- RAID 3 and 4
- RAID 5
- RAID 6
- RAID 0+1 and 1+0

Standalone

Hot swap

Cluster

RAID 0

RAID 1

RAID 5

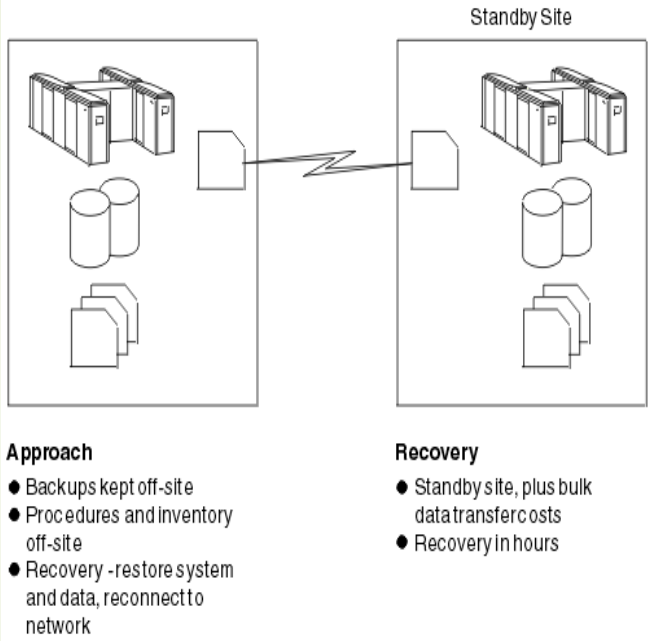
RAID 0+1

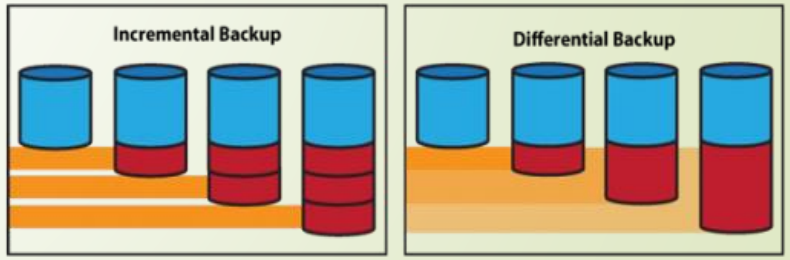
Drives and Data Storage – Redundant Array of Independent Tapes (RAIT) Levels

- Used with tape vaulting to make multiple copies of tapes for backup and recovery
- Relays on robotic mechanisms to automatically transfer tapes between the storage and the drive mechanisms

System Resilience and Fault Tolerance Requirements – Backup and Recovery Systems

- Electronic Backups
  - Full
  - Incremental
  - Differential
  - Electronic Vaulting
  - Remote Journaling
- Off-Site Storage (RTO 3-5 days)
- Tape vaulting
  - Tape rotation methods
- Database Shadowing
- High Availability Options
- Software Escrow
- Hardcopy Data





Archive Bit

Example from a $MFT record

$FILE_NAME 1:

ParentSequenceNo: 1

CreationTime (CTime): 2013-06-24 21:10:46:101:7529

LastWriteTime (ATime): 2013-06-24 21:10:46:101:7529

ChangeTime (MTime): 2013-06-24 21:10:46:101:7529

LastAccessTime (RTime): 2013-06-24 21:10:46:101:7529

AllocSize: 0

RealSize: 0

Flags: archive **(ARCHIVE BIT VALUE)**

NameLength: 9

NameType: DOS+WIN32

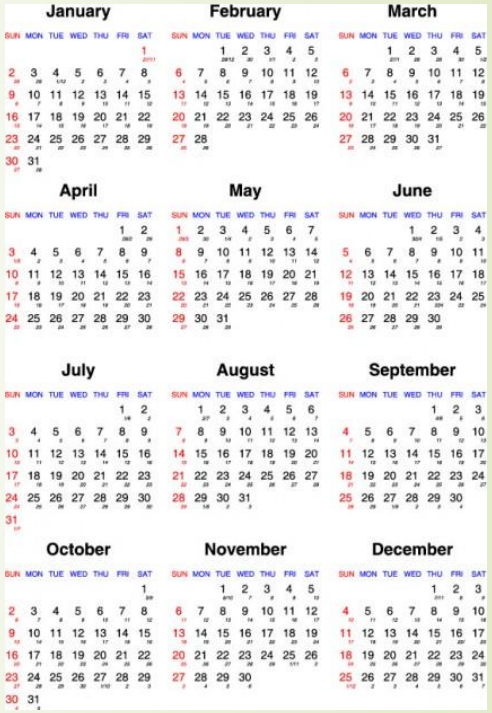
NameSpace: 8

FileName: newfile.txt

ParentReferenceNo: 77464

System Resilience and Fault Tolerance Requirements – Staffing for Resilience

- Audits, Drills, Exercises, and Testing
  - May be paper based to review the practical effectiveness of physical and procedural measures
  - Interviews with staff
  - Conducted annually or when any significant breach of security or change in the risk indicates that it may be needed



The Disaster Recovery Process (DRP)

- Is the process of restoring services from a contingency state
- Personnel Safety Top Priority (Safety Trumps Everything)
- There must be an initial response that assesses the situation
  - The initial response needs to work quickly to determine the need for an alternate site and to gauge the safety of the workforce

DRP Steps

- Respond
- Activate Team
- Communicate
- Assess
- Reconstitution

The DRP - Documentation

- Document the DRP plan once recovery strategies have been developed
  - Should be detailed enough to perform the recovery
  - Should be stored offsite (i.e. recovery location)
  - Should be tested and updated as needed
  - Use version control
- Event Management Process
  - Is about communication and response during non-disaster and disaster events
  - Is triggered by an event which is anything that either already has or has the potential to cause a significant organizational interruption

The DRP - Response

- A central communications group (i.e. an Emergency Operations Center [EOC]) is responsible for initiating communications to those who:
  - Must respond to the event
  - Are impacted by the event

- Event Management Plan:
  - Is part of the Business Continuity Plan (BCP) & DRP
  - Identifies who:
    - Is authorized to declare a disaster
    - How a declaration is done
    - When the decision to 'declare' is made
    - How it will be communicated to the teams that need to respond

The DRP - Executive Emergency Management Team

- Made up of senior executives
- Responsible for overall recovery of organization
- Not concerned with day to day operations
- Responds to and assists in the resolution of issues which need their direction
- Spokesperson for the organization to the media
- Decision maker on how the organization will manage the business impacts of the event

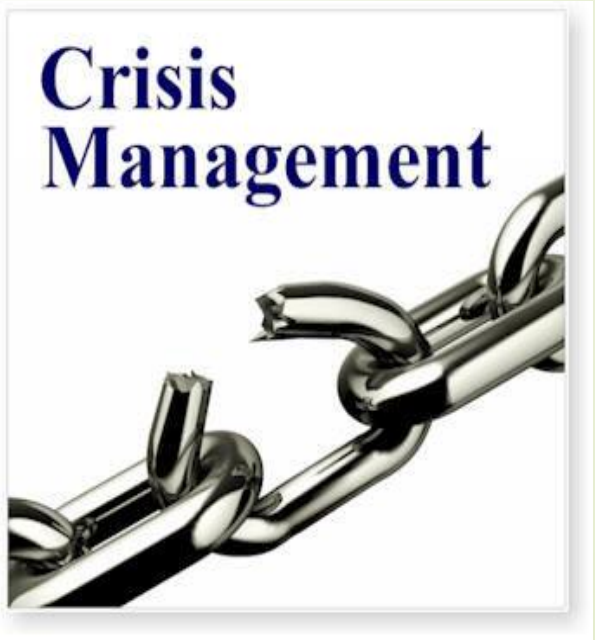
The DRP - Executive Emergency Management Team

- Executives are concerned with strategic issues not with tactical delivery

- Crisis Management versus Crisis Leadership
- Managing vs. Leading
- React vs. Anticipate
- Short term vs. Long term
- Process vs. Principles
- Narrow focus vs. Wide focus
- Tactical vs. Strategic

Crisis Management Plan

- Provides effective coordination between managers in the event of a disruptive event
- Consists of:
  - Crisis Communications Plan
  - Call Trees
  - Emergency Operations Center
  - Vital Records



Considerations - Vital Records

- Records needed to rebuild the business are stored offsite
  - Secure location accessible after a disaster
- Common vital records (Legal)
- Common vital records (Business)

The DRP - Emergency Management Team

- Team members report directly to the command center
- Have responsibility to oversee the recovery and restoration process
- Responsible for communicating the recovery status to the executive management team and making necessary decisions to support the recovery efforts
- Objectives and functions include:
  - Preliminary assessment of damage
  - Notify senior management on current status
  - Declare the disaster if necessary
  - Initiate the plan
  - Organize and control the command centers
  - Organize and provide administrative support
  - Administer and direct the problem management function

The DRP – Personnel and Communications

- Human resource issues need to be addressed depending on the disaster and may include:
  - Providing temporary location of family
  - Facilitating dependent care services
  - Providing cash advances to provide for family needs
- Administrative support do things no one else has time to do
  - Answering phones
  - Ordering food
  - Other administrative and personnel functions
- Communications
  - Notify emergency team members listed on call tree
  - Notify stakeholders
  - Notify customers or clients

The DRP – Assessment, Restoration, and Training

- An organization's people will determine if a continuity plan work or not:
  - It is the people who know the business processes
  - People create/document the recovery process
  - People test and maintain the plans
  - It is people who will be impacted by the event
  - The same people will recover the organization

Test Plan Review

- Demonstrates effectiveness, trains personnel in recovery operations, informs planner if updates are needed
- Types of tests
  - Checklist Test (a.k.a. consistency)
  - Tabletop Exercise/Structured Walk-Through Test
  - Walk-Through Drill/Simulation Test
  - Functional Drill/Parallel Test
  - Full interruption/Full-Scale Test
    - Partial interruption also exists

Test Plan Review – Update and Maintenance of the Plan

- After each exercise and after each material change to production systems
- Formal audit should be conducted annually
- Produce reports following each exercise
  - Provide to internal auditing for review
- Use version control to ensure use of current version
- Distribute to BCDR team

Additional Types of Plans

- Continuity of Operation Plan (COOP)
- Business Recovery Plan (BRP)
- Continuity of Support (CSP)
- Crisis Communication Plan (CCP)
- Cyber Incident Plan (CIP)
- Occupant Emergency (OEP)
- Fire Drills

Update and Maintenance of the Plan – Transitioning from Project to Program

- The Contingency Planning Program is designed to serve as an aid in developing and maintaining viable organizational function contingency plans
  - Is an ongoing process
    - Tasks are repeated on a regular basis
    - Has annual requirements to remain in compliance
  - Provides for the continuation of the company's critical organization functions in the event of an interruption
  - Assists and prepares various areas of the company to document and exercise emergency response and recovery plans

BCP/DRP Mistakes

- Lack of management support
- Lack of business unit involvement
- Lack of prioritization among critical staff
- Improper scope
- Inadequate communications management
- Inadequate supply chain Management
- Incomplete Crisis Management Plan
- Lack of Testing
- Lack of awareness and training
- Failure to keep the plan up to date

Update and Maintenance of the Plan – Roles and Responsibilities

- Organizational Contingency Planning Group
  - Develops, implements, and maintains the business contingency planning program
  - Provides leadership and guidance
  - Assist management in achieving timely recovery
- Business Continuity Planner
  - Focal point for company in any situation involving contingency planning or emergency response

Special Recovery Teams

- Executive Emergency Management Team
- Emergency Management Team (recovery management team)
- Damage Assessment Team
- Emergency Response Team (Backup Activation Team)
- Backup Operations Team
- Restoration/Salvage Team
- Primary Site/Service Reactivation Team

Executive Succession Planning

- Maintains a constant decision making capability
- Identifies the next in line to make decisions should an executive be unavailable regardless of the purpose

Business Continuity and Other Risk Areas

- The context of the overall risk management framework includes other risk management areas such as:
  - Physical security
  - Records management
  - Vendor management
  - Internal audit
  - Financial risk management
  - Operational risk management
  - Regulatory/compliance

Business Continuity and Other Risk Areas – Implementation and Operation of Perimeter Security

- The primary goal of a physical security protection program is to:
  - Control access into the facility
    - Use defense-in-depth strategies
- The key to a successful system is the integration of people, procedures, and equipment into a system that protects the target from the threat and the system itself has elements that falls into the essence of:
  - Deter
  - Detect
  - Delay
  - Respond

Implementation and Operation of Perimeter Security – Gates and Fences

- Barriers are meant to impede or deny access until a security team can respond and may be:
  - Natural (i.e. a river)
  - Manufactured (i.e. a wall)

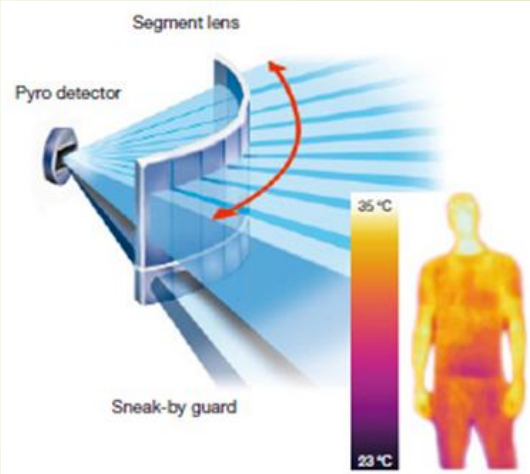
- Fence construction
  - Perimeter Walls and Fences (Heights)
    - 3 to 4 ft (1 m): Deters casual trespassers
    - 6 to 7 ft (2 m): Too hard to climb easily
    - 8 ft (2.4 m) w/ 3 strands barbed wire(top guard): Deters intruders
    - Most fencing is largely a psychological deterrent
  - Perimeter Intrusion Detection and Assessment System (PIDAS)

Implementation and Operation of Perimeter Security – Gates and Fences

- Vehicular Gates
  - Class I: residential gate operation
  - Class II: commercial (parking lot or garage)
  - Class III: industrial or limited access (warehouse, factory, loading dock)
  - Class IV: restricted access requiring security personnel (prison, airport)

Implementation and Operation of Perimeter Security – Perimeter Intrusion Detection

- Infrared Sensors
  - Passive Infrared Sensors (PIR or PID)
  - Active Infrared Sensors
- Microwave
- Coaxial Strain-Sensitive Cable
- Time Domain Reflectometry (TDR) Systems
- Video Content Analysis and Motion Path Analysis



Implementation and Operation of Perimeter Security – Lighting

- Types of lighting used for security systems
  - Continuous lighting (most common)
  - Standby lighting (automatically or manually turned on)
  - Movable lighting (movable searchlights or lighting)
  - Emergency lighting (backup to any of the previous)

Lumen=1 candle
Footcandle=1 lumen/sqft
Lux=1 lumen/sq meter

- Types of lights used in protected areas
  - Fluorescent (highly efficient and cost effective, temperature sensitive, not good for outdoors)
  - Mercury vapor (bluish cast, preferred, extended life, take time to warm up)
  - Sodium vapor (soft yellow, more efficient than mercury, good for fog)
  - Quartz lamps (produce daylight quality for high visibility
  - Fresnel lamps (lighthouses/search lights)

- Infrared Illuminators allow night surveillance without using additional lighting

Access Control

- An Access Control System (ACS) ensures that only authorized personnel are permitted inside a controlled area
- Basic components:
  - Card reader
  - Electric Locks
  - Alarms
  - Computer systems to monitor and control the ACS
- Card Types
  - Magnetic stripe
  - Proximity card
  - Smart cards
- Access Control Head End
  - Is the application SW housed in the CPU and provides the intelligent controller where all ACS activity is monitored, recorded, commanded, and controlled by the operator

Access Control – Closed-Circuit Television (CCTV)

- Is a collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events
- Is integrated into the overall security program
- Security functions:
  - Surveillance
  - Assessment
  - Deterrence
  - Evidentiary Archives

CCTV - Cameras

- Fixed position cameras
- Pan Tilt Zoom (PTZ)
- Ability to be recorded (DVR or NVR)
  - DVR uses internal storage where a NVR uses TCP/IP and network storage
- CCTV displays
  - Fixed
  - Autoscan
  - Multiplex
- Alarm monitoring (i.e. human intervention)

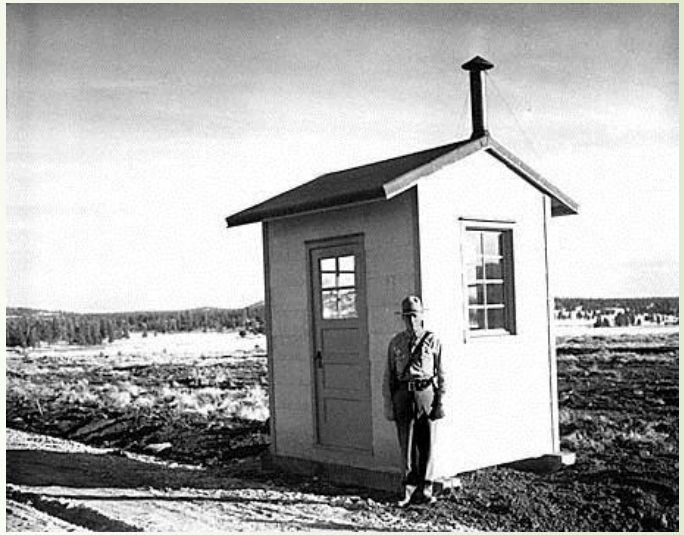
CCTV – Lens Selection

- Depth of Field: Area in focus
  - Good light allows for a larger depth of field (small aperture)
  - Low light reduces depth of field (wide aperture)
- Focal Length: 2.8-4.3mm for wide angle and 8mm and above for zoom
- CCD (Charged Coupled Device)
- Size of aperture is called an F-stop
  - Small F-stop (e.g. f/4) is a large aperture
  - Large F-stop (e.g. f/32) is a small aperture

60mm lens at F4

60mm lens at F32

Guards



- Guard post
  - Gate control
  - Shift overlap
  - Glare protection
- Checking and escorting visitors on Site
  - Defend against unauthorized access
- Managing deliveries to the Site
  - Different levels of security
    - Reception areas, CCTV, management of entry and exit points

Dogs

- Good perimeter defense in a controlled area
- Deterrent and detective measure
- Dogs present a legal liability
  - Most trained dogs will not attack if the suspect is stationary
  - Most victims of dog attacks do not know this

Shared Tenancy and Adjacent Buildings, and Shared Demarc

- Shared Tenancy and Adjacent Buildings
  - Difficult for territorial reinforcement
  - Lax security in one company or building can impact others
  - Wireless systems may be causing interference or provide a location for monitoring
- Shared demarcs require Strong physical access control

Access Control – Internal Security

- Interior Intrusion Detection Systems provide an additional layer of protection within the facility
  - Balanced Magnetic Switch (BMS)
  - Motion Activated Cameras
  - Acoustic Sensors
  - Infrared Linear Light Beam Sensors
  - Passive Infrared (PIR or PID) Sensors
    - Dual-Technology Sensors

Internal Security – Escort and Visitor Control

- Beware of attempts to reuse old badges, stolen badges, fabricated badges or social engineering

- Mitigation methods:
  - Time based badges
  - Color coded badges for different days of the week
  - Electronic badges
  - Provide guards to escort visitors

Port Controls

- Portable devices can be used to move large amounts of data both legally and illegally
- Methods to control their use:
  - Physically disable port
    - Disconnect
    - Physically block access to it
  - Electronically lock the port
    - Disable in software

Access Control – Building and Inside Security

- Doors (includes the door, its frame and anchorage to the building)
  - Should fit snuggly in the frame
  - Doorframes and locks must be as secure as the door
  - Perimeter doors
    - Consist of hollow steel doors or steel-clad doors with steel frames
  - Exterior doors
    - Should open outward if in an inhabited area
    - Hinges should be located on the interior of restricted areas
  - Glass doors
    - Material should be of a laminate material or stronger
  - Sensitive areas should have an automatic door closing device

Building and Inside Security – Door Locks

- Electric Locks
  - Is a secure method to control a door
  - An electronic lock actuates the door bolt
- Electric Strikes
  - The door and bolt remain stationary and the strike is retracted
- Magnetic Locks
  - Power is applied to the magnets to hold the door closed
  - Per the U.S. Life Safety Codes
    - Magnetic locks require an emergency manual override button
      - When someone approaches the door in the exit direction
- Anti-Passlock
  - Used in high security areas and users must badge in and out

Building and Inside Security – Turnstiles and Mantraps

- Mantrap
  - Entry with two doors
    - First door must close and log prior to the second door opening
    - Each door must require a different form of authentication to open

- Turnstile
  - Designed to prevent tailgating
  - Allow only one person at a time to access
- Both must allow safe egress in case of an emergency
- No system should require authentication in order to exit during an emergency

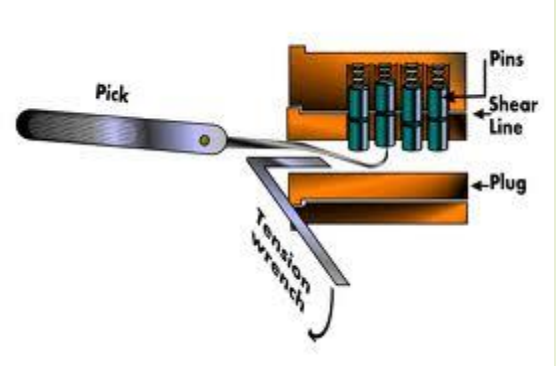
Tailgating/Piggybacking

- Bypass an access control method by following an authorized person through the entry point
- Policies should include language prohibiting employees for allowing the practice
- Beware the social engineer

Building and Inside Security – Keys, Locks and Safes

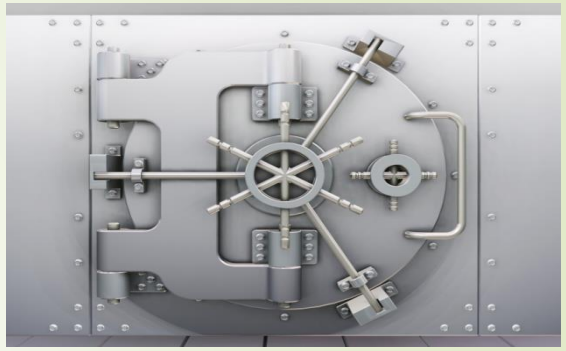
- Key locks are a basic safeguard in protecting buildings, personnel and property (i.e. doors and windows)
  - Types:
    - Rim Lock
    - Mortise Lock
    - Locking Cylinders
    - Cipher Locks
    - Hi-Tech Keys
      - Intelligent Keys
      - Instant Keys

Lock Picking



- Lock Picks
  - Tools used to depress the pin tumblers
- Key bumping
  - Shaved down key that allows the lock to be bumped thus allowing the lock to be turned
- Master key
  - Opens all locks of a certain type or series
- Core key
  - Used to change out the keying portion of the lock
- Shimming
  - Using a thin material to circumvent the lock catch

Building and Inside Security – Keys, Locks and Safes

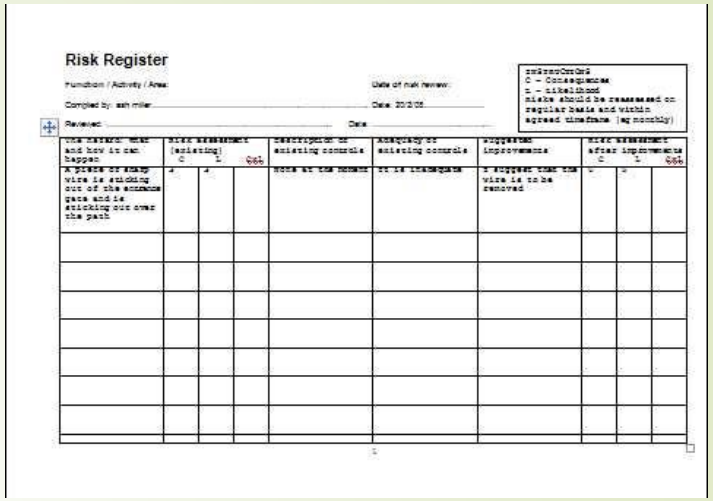


- Safes
  - Are defined as fireproof and burglarproof iron or steel chests
- Vaults
  - Are defined as a room or compartment designed for storage and safekeeping of valuables and has a size and shape that permits entrance and movement within by one or more persons
- Containers
  - Are reinforced filing cabinets that can be used to store property

Keys, Locks and Safes - Key Control

- Lack of key control is one of the biggest security risks faced by business or property owners
- Must know who has keys
- Must protect against unauthorized duplication
- Should appoint a key control manager
- Develop a policy and method for issuing and collecting keys
- All keys should remain the property of the issuing facility
- Only issue for official use by authorized individuals
- Employees must ensure keys are safeguarded and properly used

Asset Tracking


Risk Register

Function / Activity / Area:

Date of risk review:

Compiled by: ash miller

Date: 20/3/05

Reviewed:

Date:

RATING CRITERIA
C – Consequence
L – Likelihood
Risks should be reassessed on regular basis and within agreed timeframe (eg monthly)

The hazard: what and how it can happen	Risk assessment (existing) C	L	Risk	Identification of existing controls	Adequacy of existing controls	Suggested improvements	Risk assessment after improvements C	L	Risk
A piece of scrap wire is sticking out of the common gate and is sticking out over the path	4	4		Note at the house	It is inadequate	I suggest that the wire is to be removed			

- Enhances physical security
- Useful tool to analyze loss, theft, or disasters
- Supports regulatory compliance by pinpointing data location
- Tracks the relationship between customers and employees to the data and various devices that they use
- Asset and Risk Registers
  - List of assets
  - List of staff who access secure areas
    - Useful to establish possible personnel with opportunity to commit the theft

Personnel Safety

- Personnel are a great asset when designing physical and environmental security
- Mobile computing has raised issues about privacy and physical concerns when traveling
  - Privacy
    - Difference in perspective as to what falls under 'the right to privacy'
    - Privacy policy should address monitoring
  - Traveling
    - Ensuring the safety of personnel and corporate data while traveling

Personnel Safety – Traveling

- Before you travel
  - If you do not need the electronic device, don't take it
  - Do not travel with information you do not need
- Prepare your device
  - Create strong passwords
  - Change passwords as soon as you return
- While you're away
  - Avoid placing devices in checked baggage
  - Use digital signatures and encryption
- When you return
  - Change passwords
  - Examine the device for malware

Personnel Safety - Duress

- Divulging something you normally wouldn't but did under threat of harm
- Proper training is crucial to ensure personnel safety as situations can occur quickly
- Personnel with access to an asset are targets of duress
- The protection and risk of duress follows the asset and the access to the asset

Questions?

Software Development Security

(Understanding, Applying, and Enforcing Software Security)

Domain Objectives

- Understand and apply security in the software development lifecycle
- Enforce security controls in the development environment
- Assess the effectiveness of software security
- Assess software acquisition security

Systems Development Life Cycle (SDLC)

- Focuses on security at every level
- Used to plan, execute, and control a software development project
- Security plan is the first step of any SDLC model
- Multiple models of the SDLC
- Most models contain 5 basic phases:
  - Initiation
  - Development/acquisition
  - Implementation
  - Operation
  - Disposal

Systems Development Life Cycle (ISC)2

- Project initiation and planning
- Functional requirements definition
- System design specifications
- Develop and implementation
- Documentation and common program controls
- Testing and evaluation control (certification and accreditation)
- Transition to production (implementation)

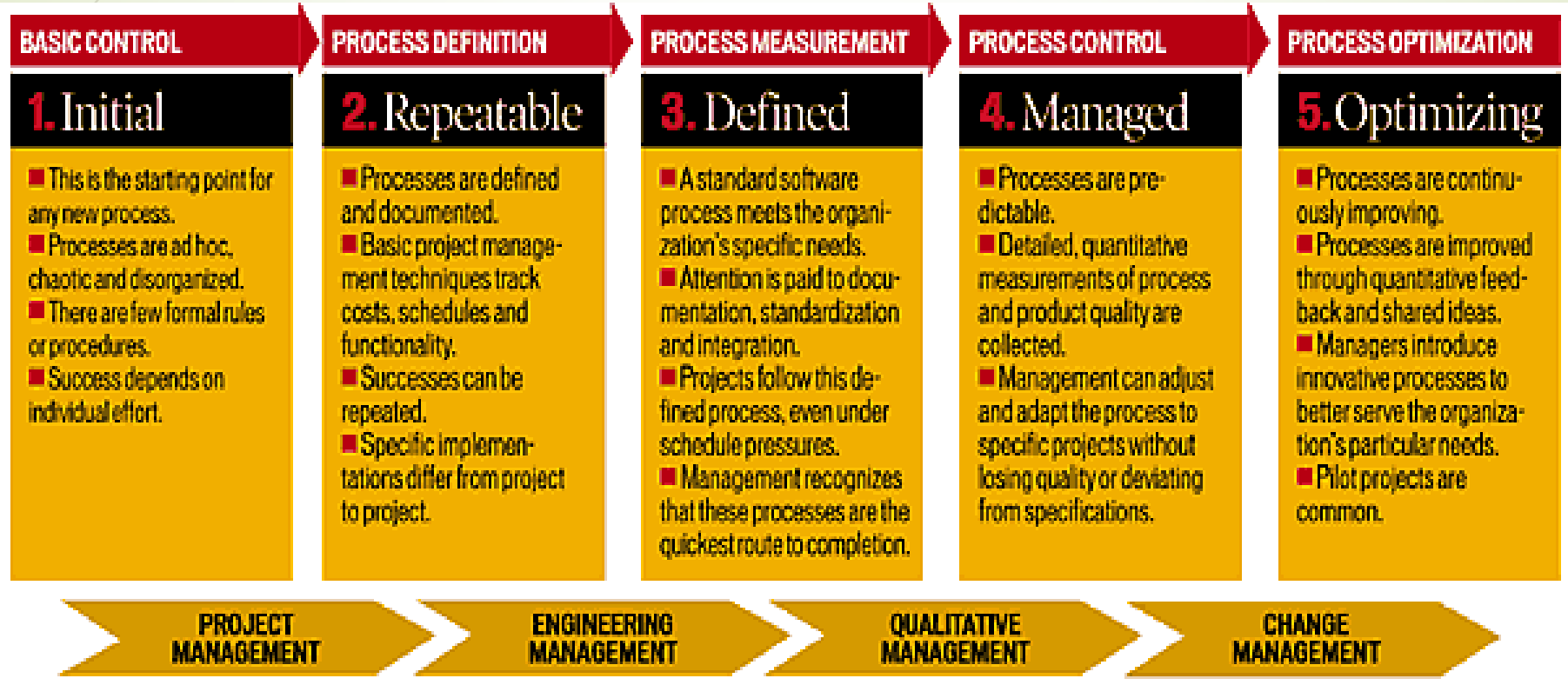
Systems Life Cycle (SLC)

- Extends past the SDLC to include two additional layers
  - Project initiation and planning
  - Functional requirements definition
  - System design specifications
  - Develop and implementation
  - Documentation and common program controls
  - Testing and evaluation control (certification and accreditation)
  - Transition to production
  - Operations and maintenance support (post-install)
  - Revisions and system replacement

Capability Maturity Model (CMM)

- Sometimes called “software capability maturity model”
- Focuses on Quality Management
- Provides policies, procedures, guidelines, and best practices to provide a standardized approach to software development
- Addresses security and systems integration
- Takes a proactive approach rather than a reactive approach to programming
- Made up of 5 Process Maturity Levels (initial, repeatable, defined, managed, optimizing)

Capability Maturity Model (CMM)



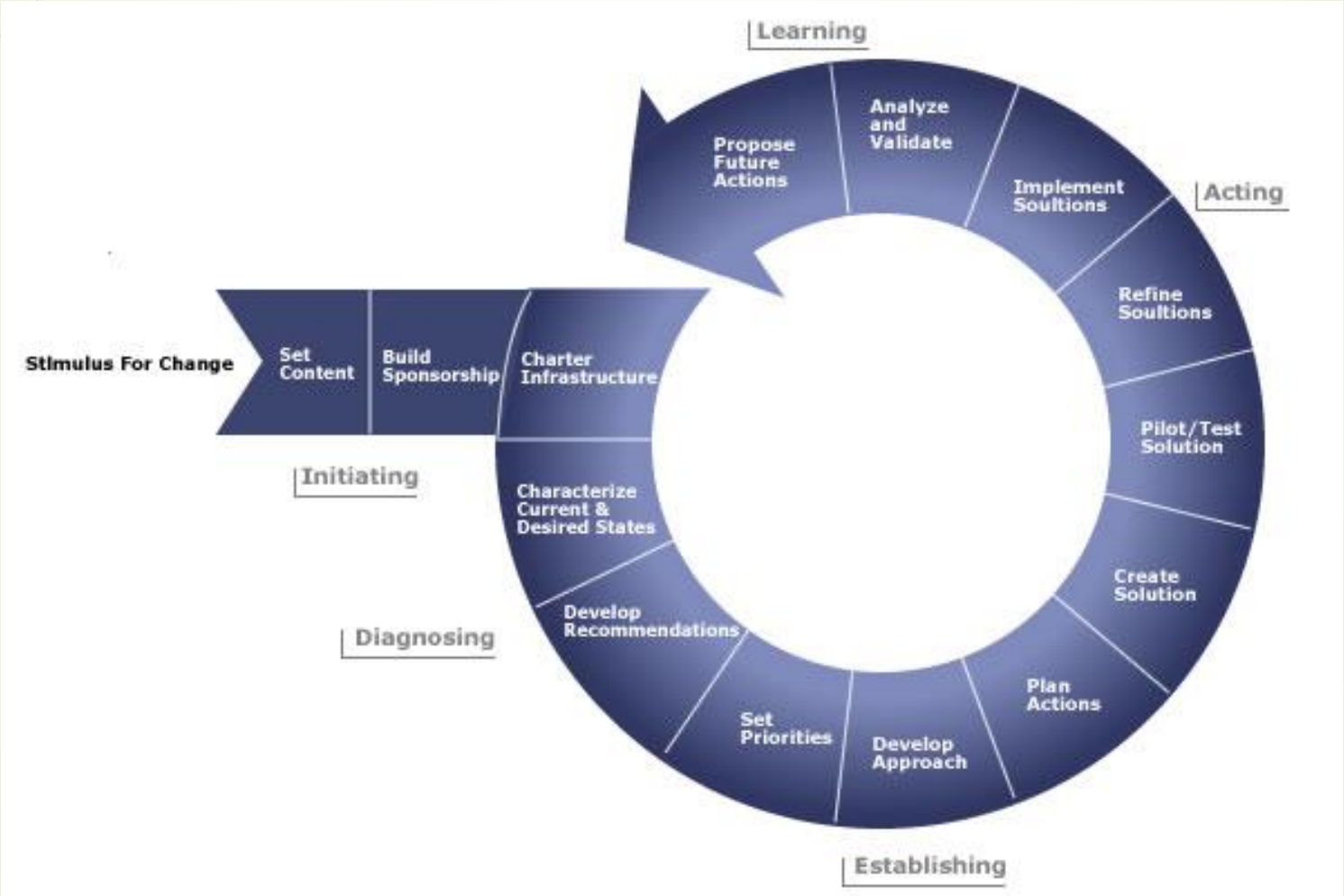
IDEAL MODEL

- Initiating
  - Outline business reasons behind the change
- Diagnosing
  - Analyze the state of the organization
  - Make recommendations for change
- Establishing
  - Develop a plan of action to achieve changes

IDEAL MODEL

- Acting
  - Develop solutions, test, refine, implement
- Learning
  - Analyze efforts to determine if goals were achieved
  - Lessons learned

IDEAL MODEL


Learning
Analyze and Validate
Propose Future Actions
Implement Soultions
Acting
Refine Soultions
Stimulus For Change
Set Content
Build Sponsorship
Charter Infrastructure
Pilot/Test Solution
Initiating
Characterize Current & Desired States
Create Solution
Develop Recommendations
Diagnosing
Plan Actions
Set Priorities
Develop Approach
Establishing

Control and Separation of Environments

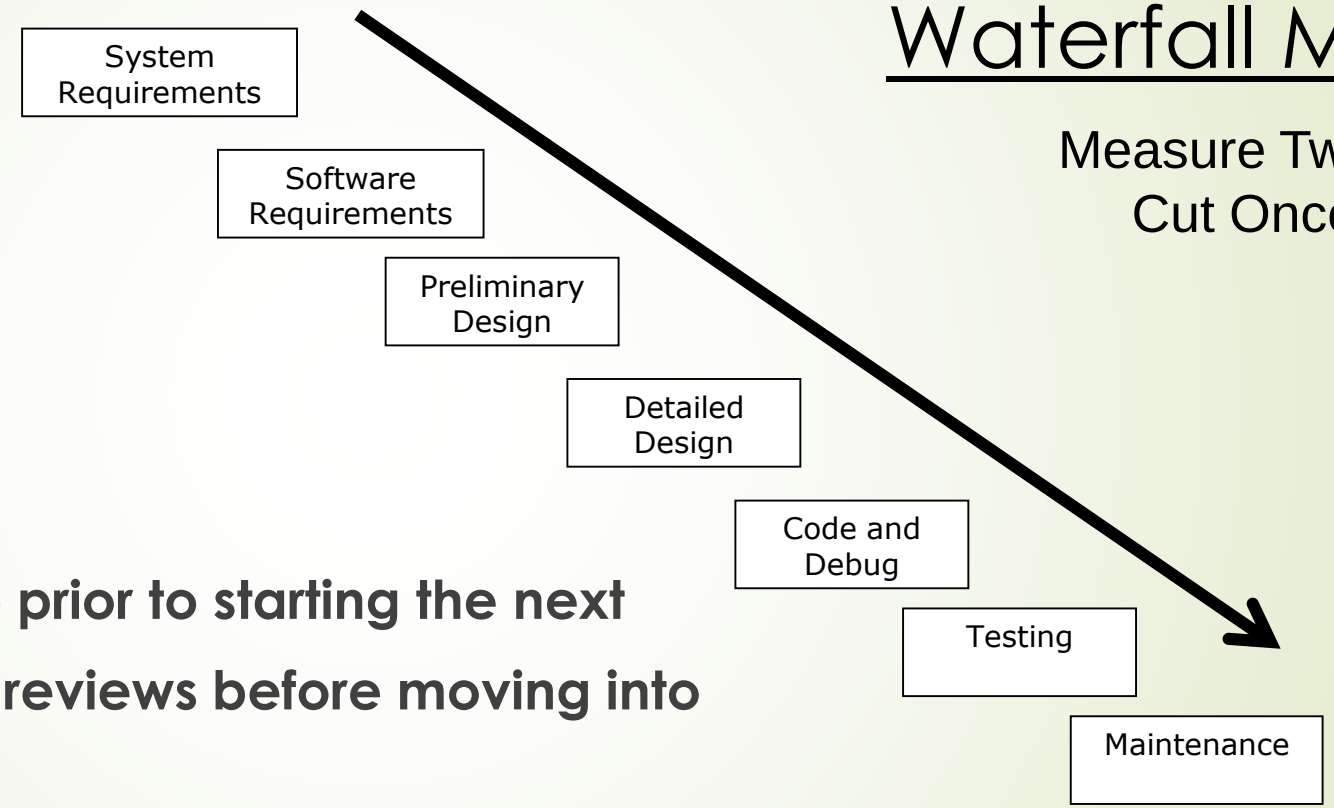
- Three environments exist:
  - Development
  - Quality Assurance/Staging
  - Application (Production/users)

- To separate environments:
  - Physical Separation
  - Access Control Lists
  - Content Dependent Access Controls
  - Role Based Restraints
  - Accountability
  - Separation of Duties

Software Development Methods

Waterfall Method

Measure Twice,
Cut Once



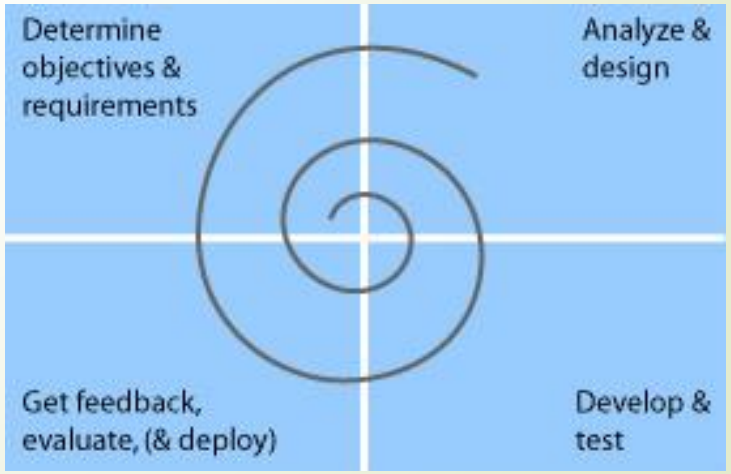
- **Finish one stage prior to starting the next**
- **Requires formal reviews before moving into the next phase**
- **Paradigm for non-iterative models**
- **Non-iterative are more secure**

Structured Programming Model

- Structured Programming Development
  - Non-iterative
  - Widely known model taught in almost all academic systems development courses
  - Promotes discipline, allowing introspection, and provides controlled flexibility
  - Requires refined processes and modular development
  - Each phase subject to review and approval
  - Allows for security to be added in a formalized, structured approach

Spiral Method

- Non-iterative
- Estimated costs and schedules are revised at the end of each risk assessment
- Decision to proceed/cancel project is revisited after each risk assessment
- Nested waterfall phases
  - Each phase has 4 sub phases
  - Phases based on Deming PDCA
  - Plan, do, check, act



Clean Room

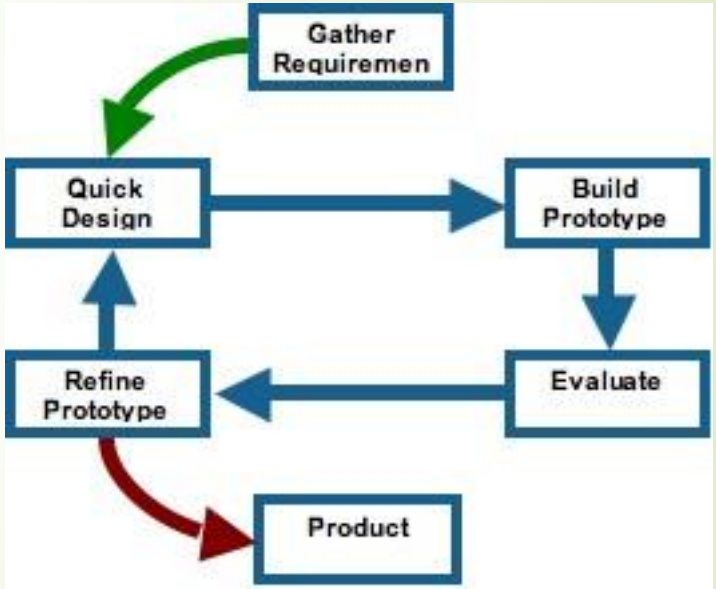
- Non-iterative
- Write good code the first time
- Controls defects in software
- Quality achieved through design versus testing and remediation
- Focus is on defect prevention rather than defect removal

Iterative Models

- Allow for successive refinements
  - Requirements
  - Design
  - Coding
- Change control mechanism implemented
- Makes security more difficult
- Project scope may be exceeded by requirement changes

Prototyping

- Prototyping
  - Iterative
  - Developed to combat the weaknesses of the waterfall model
  - Refine prototype until acceptable
  - 4 Step Process:
    - Initial Concept
    - Design and Implement Initial Prototype
    - Refine Prototype
    - Complete and Release



Modified Prototype Model

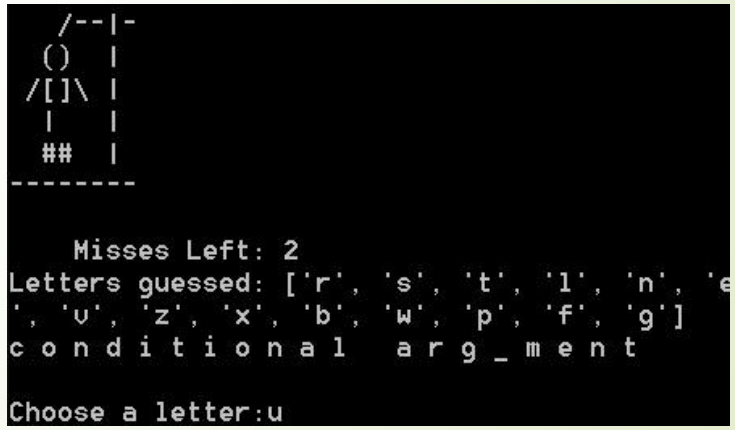
- Modified Prototype Model (MPM)
  - Iterative
  - Ideal for web application development
  - Allows for basic functionality to be deployed in a quick time frame
  - Maintenance phase begins after the deployment
  - Application evolves as the environment changes (not frozen in time)

RAD / JAD

- Rapid Application Development (RAD)
  - Iterative
  - Rapid prototyping within strict time limits
  - Can be a disadvantage if decisions are made too quickly
- Joint Application Development (JAD)
  - Iterative
  - Management process that allows developers to work directly with users
  - Key players communicate at key phases of development

Exploratory Model

- Requirements built on what is available
- Built on assumptions as to how the system might work
- Consists of planning and trying different designs before development
- Not cost-effective
- Results in less-than-optimal systems
- Iterative

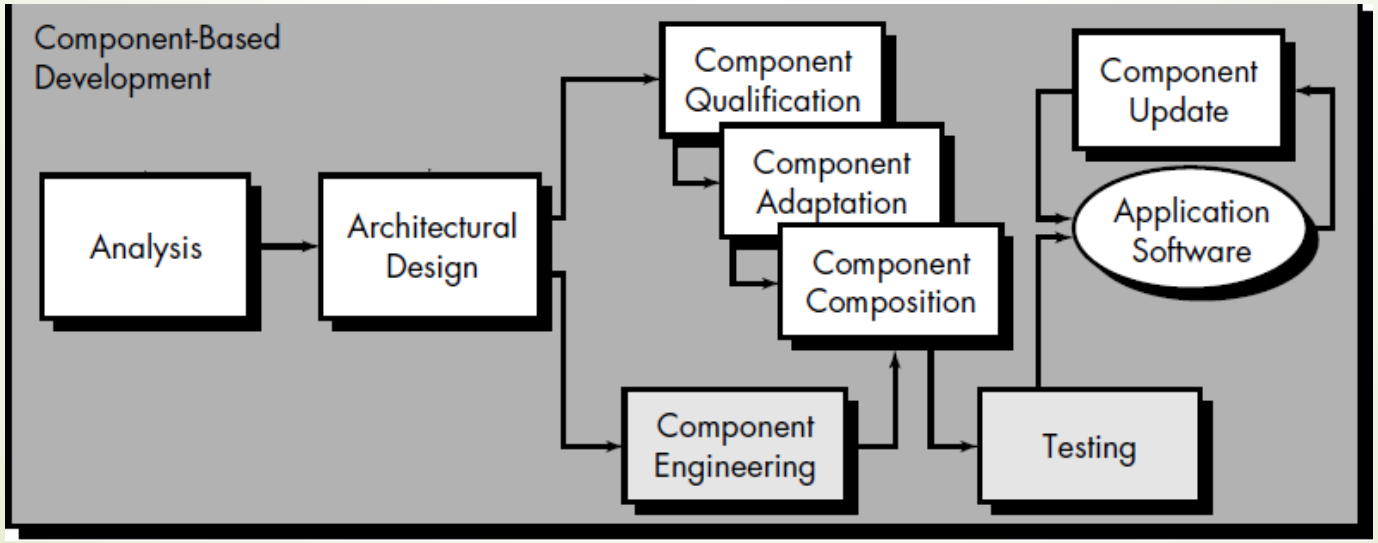


Computer-Aided Software Engineering (CASE)

- Tools using computers and computer utilities to support software engineering tasks and activities in the process of developing software
- Examples are compilers, assemblers, linkers, translators, loaders/debuggers, program editors, code analyzers, and version control mechanisms
- When the CASE tools are integrated: ICASE

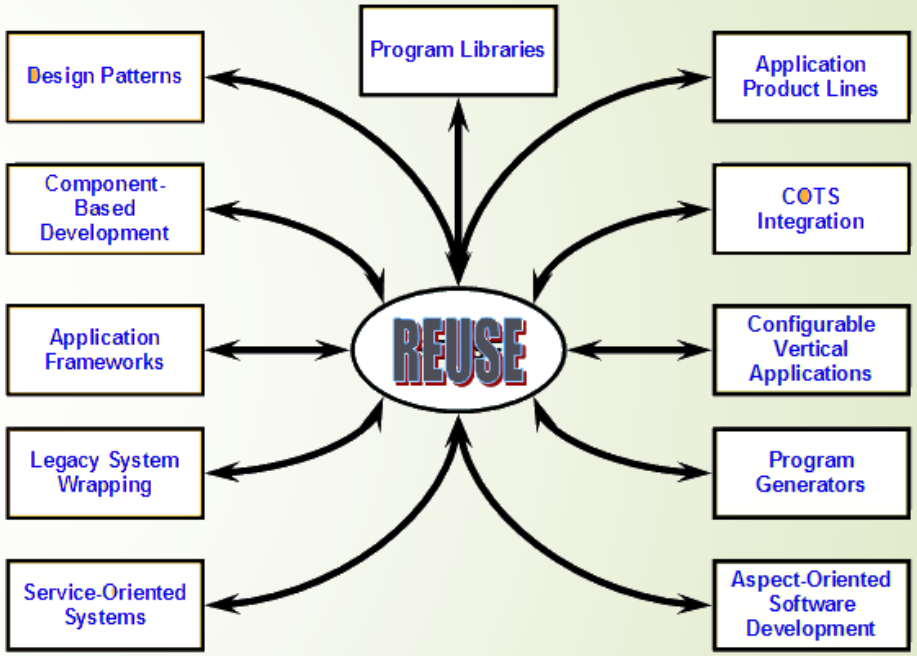
Component Based Model

- Component Based Development
  - Involves using standardized building blocks to assemble, rather than develop, an application
  - May be a security advantage as the components have previously been tested for security
  - Similar to Object Oriented Programming (OOP)



Reuse Model

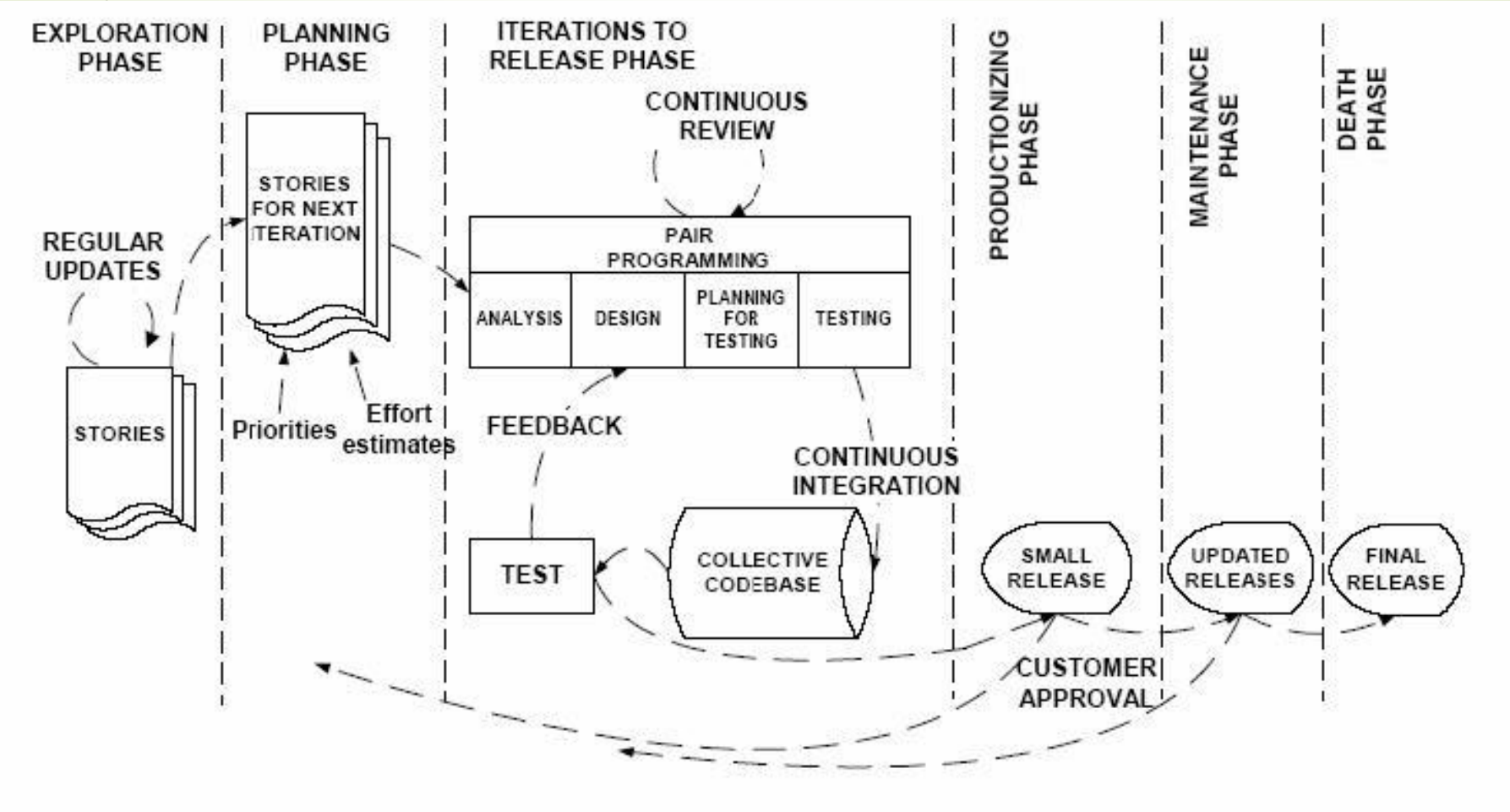
- Reuse Model
  - Built from existing components
  - Best suited for projects using object oriented development … because objects can be exported, reused, and modified
  - Libraries of software modules are maintained to be copied for use in any system



Extreme Programming (XP)

- Extreme Programming
  - Based on simplicity, communications, and feedback
  - Relies on subprojects of limited and defined scope with programmers working in pairs
  - Works best with a dozen or fewer programmers
  - Core practices:
    - Planning
    - Paired Programming
    - 40 hour workweek
    - Total customer involvement
    - Detailed test procedures

Extreme Programming



Agile Method

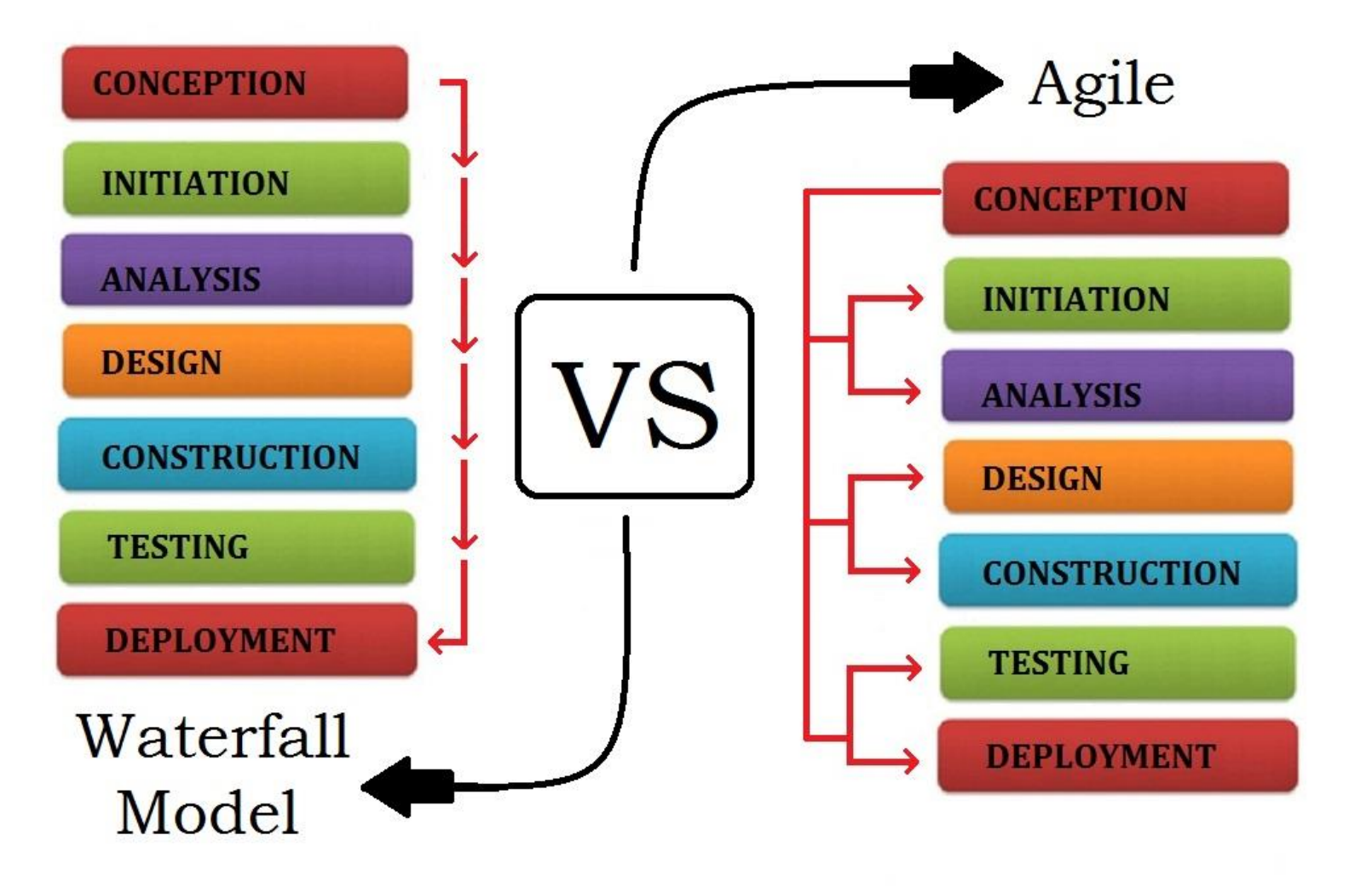
- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan
- More flexible
- Fast turnaround
- Strong communications
- Customer involvement
- Methods include scrum and extreme programming

Agile Versus Waterfall

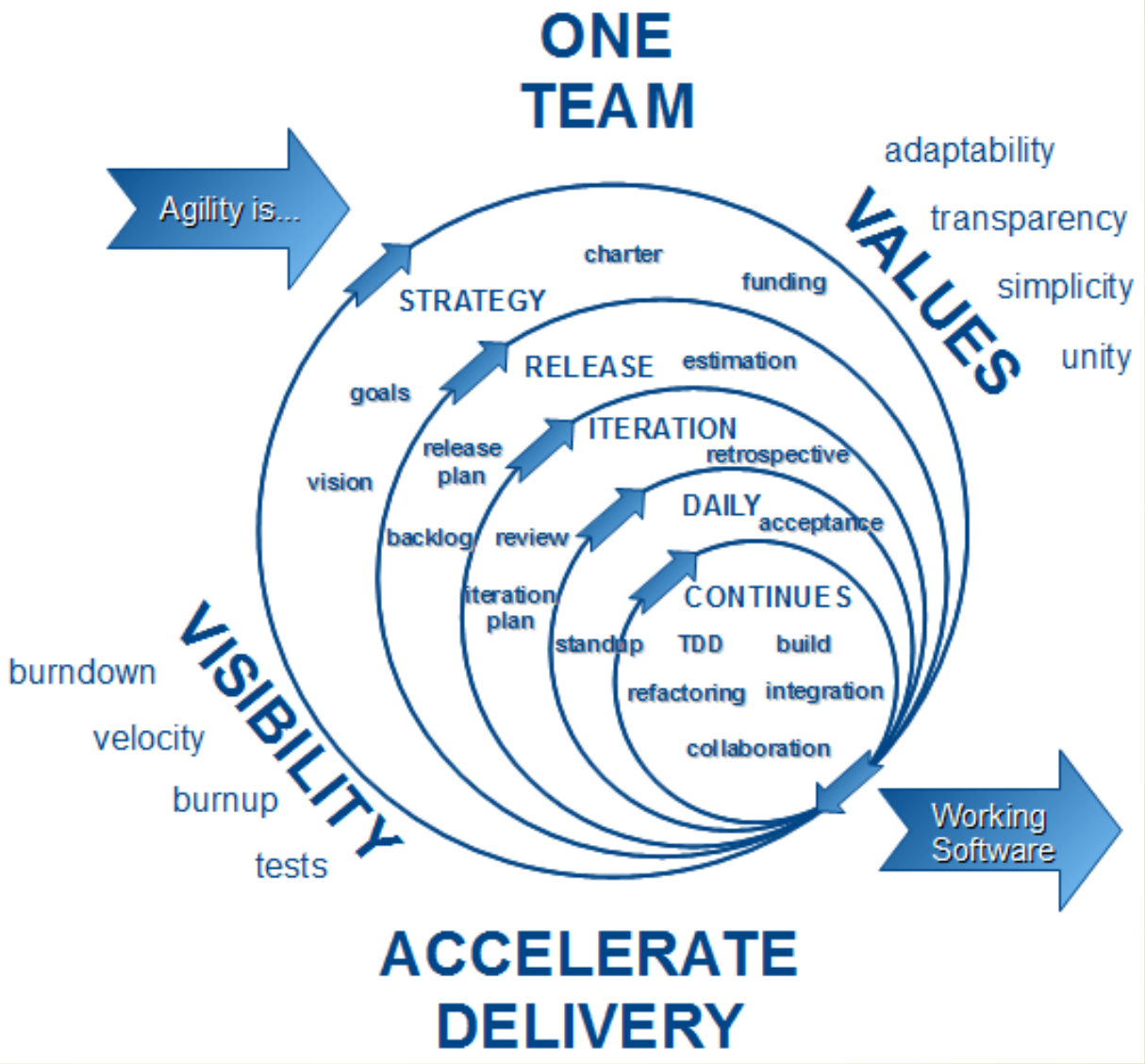
Agile Versus Traditional Waterfall

Metric	Waterfall	Agile
Planning scale	Long-term	Short-term
Distance between customer and developer	Long	Short
Time between specification and implementation	Long	Short
Time to discover problems	Long	Short
Project schedule risk	High	Low
Ability to respond quickly to change	Low	High

Waterfall versus Agile

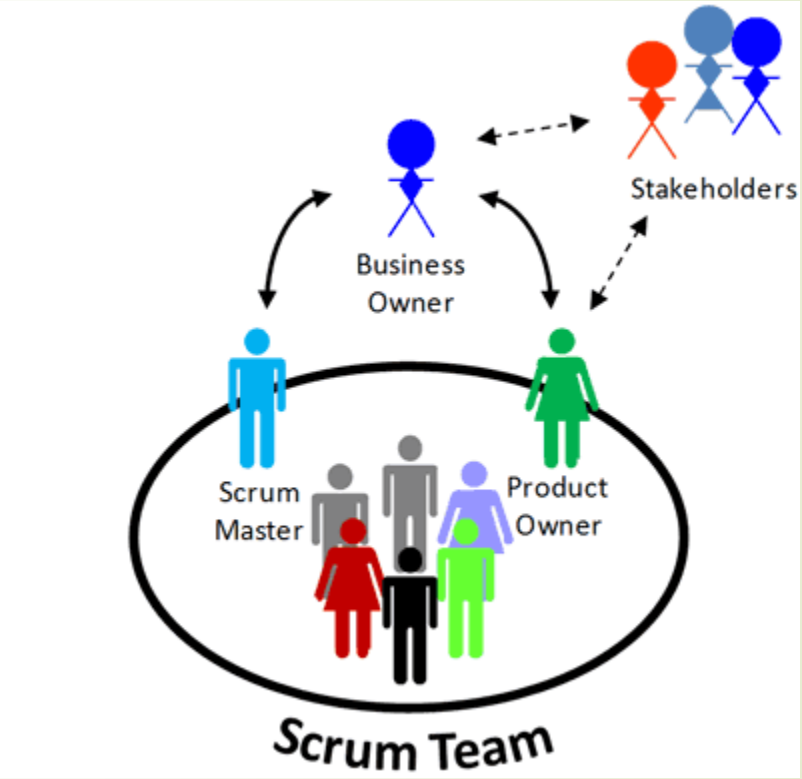


Agile Method



Scrum Development Model

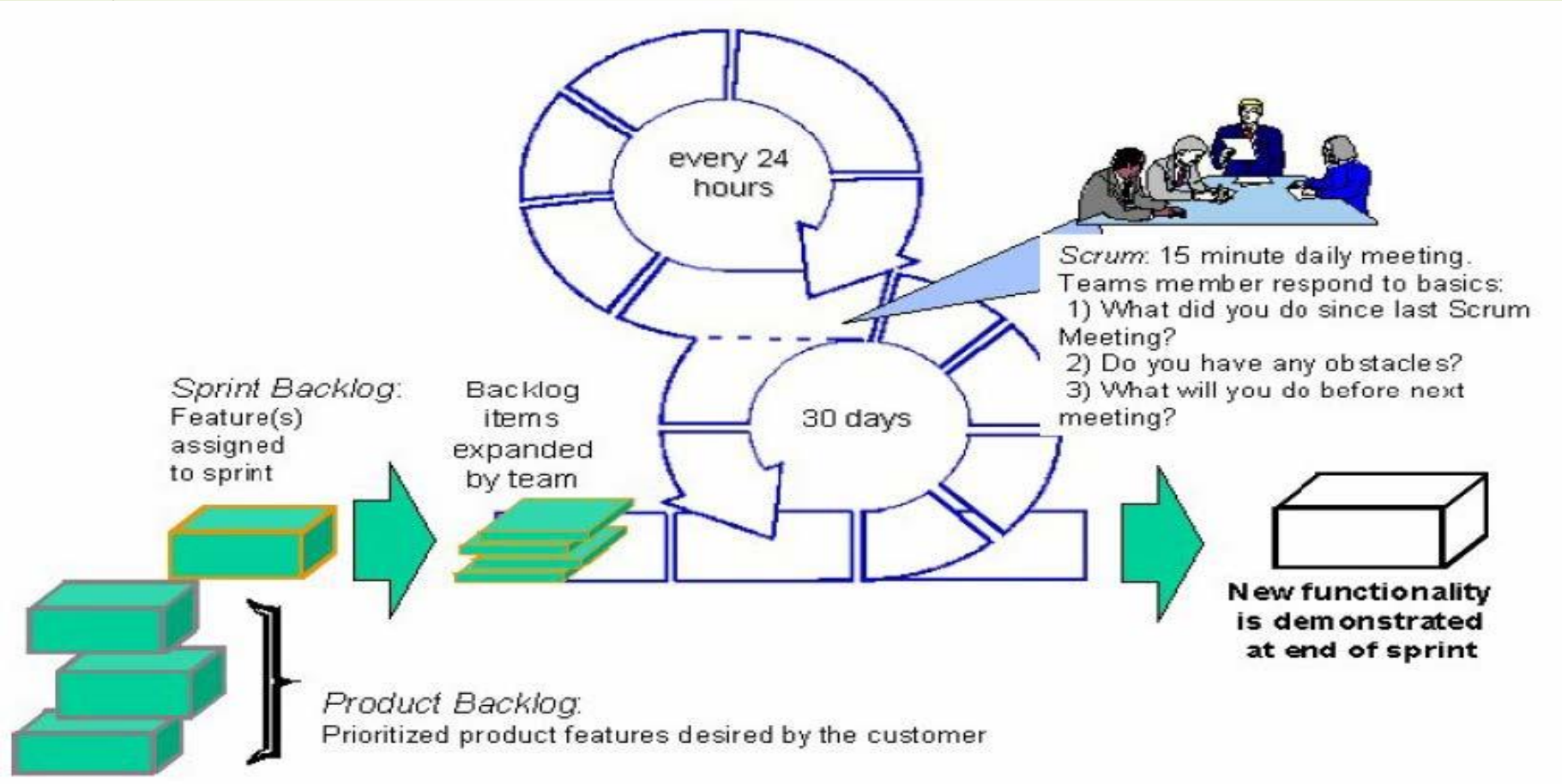
- Small teams of developers called scrum teams
- Scrum master supports the scrum team
- Product owner makes major decisions
- The teams take the project from start to finish, handing off similar to rugby



Key Scrum Practices

- Product Backlog (List of all changes to be made –maintained by Product Owner)
- Sprints (30 days in length)
- Sprint Planning Meeting (goals and how-tos are formulated)
- Sprint Backlog (list of features assigned to a particular sprint)
- Daily Scrum (daily meeting to keep track of progress)

Scrum Practices

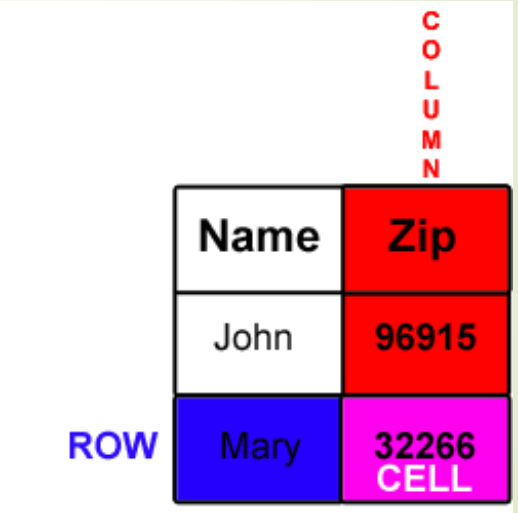


Database Terminology

- Record - collection of related data items
- Table/File - collection of records of the same type
- Database - cross referenced collection of data
- DBMS - manages and controls the database
- Relationship - related records within tables
- Tuple / Record (row)
- Attribute / Field (column)
- Cardinality - number of rows in a relationship

Database Terminology

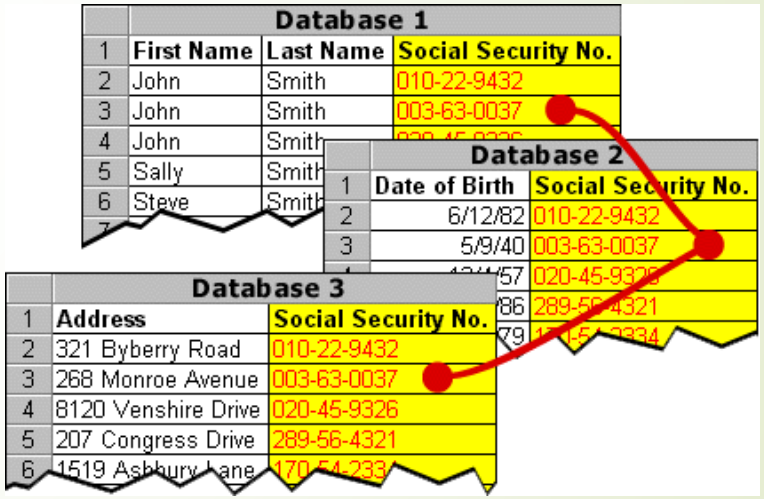
- Degree - number of columns
- Cell - intersection of a row and column
- Element – data within the cell
- Candidate Key - attributes identifying a record
- Primary Key - unique identifier
- Foreign Key - attribute related to another table
- View - virtual table
- Schema - DB structure



Database Management System (DBMS) Architecture

- Model should provide for:
  - Transaction persistence
  - Fault tolerance and recovery
  - Sharing by multiple users
  - Security controls

- Database Management Models
  - Hierarchical
  - Network
  - Relational



Databases & Database Management Systems (DBMS)

- Flat File - database in a single table
- Hierarchical - records structured in a hierarchy
  - Legacy Systems
- Distributed - data in more than 1 DB
- Relational - two dimensional tables
  - Interrelationships (tables mapped)
- Object-Oriented
  - Creation of data as objects
  - For complex applications (CAD, video, etc.)

Lock Controls (ACID)

- Database transaction requirements for developing database systems
  - Atomicity
  - Consistency
  - Isolation
  - Durability

Database Integrity

- Three types of integrity checks:
  - Semantic (structural enforcement)
  - Referential
    - Foreign Keys reference Primary Keys
    - Cascading Update/Delete
  - Entity
    - Tables must have a Primary Key
    - Primary Key columns must be unique and not null

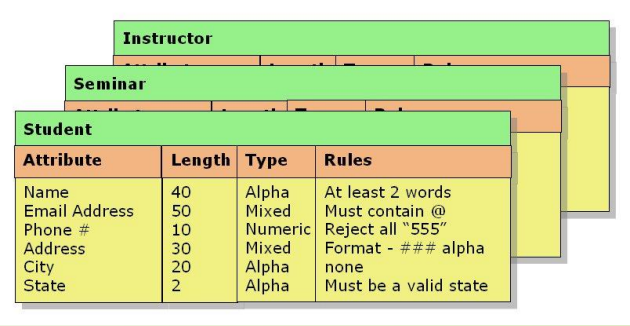
Database Normalization

- Normalize: Reduces duplicated data and makes the structure more consistent
  - 1NF (first normalization form) each column type is unique. Data is divided into tables.
  - 2NF (2nd normalization form) move data that is partially dependant on primary key to new table
  - 3NF (3rd normalization form) considered normalized. Remove data not dependent on primary key
  - BCNF (Boyce-Codd Normal Form) all tables only have one primary key
  - 4NF (multi-valued dependencies (reduce columns))
  - 5NF (when the data can no longer be reconstructed from smaller data forms(reduce data redundancy))

- Denormalize: can increases data access in a distributed database

Data Dictionary

- Used by the RDBMS as a reference guide to the data stored in the database files
- A user retrieves data from views stored in the Data Dictionary
- The Data Dictionary stores:
  - names of tables, space definitions, views, indexes, clusters, synonyms, etc.
  - user names having access to the DB
  - rights and privileges that have been granted



Structured Query Language (SQL)

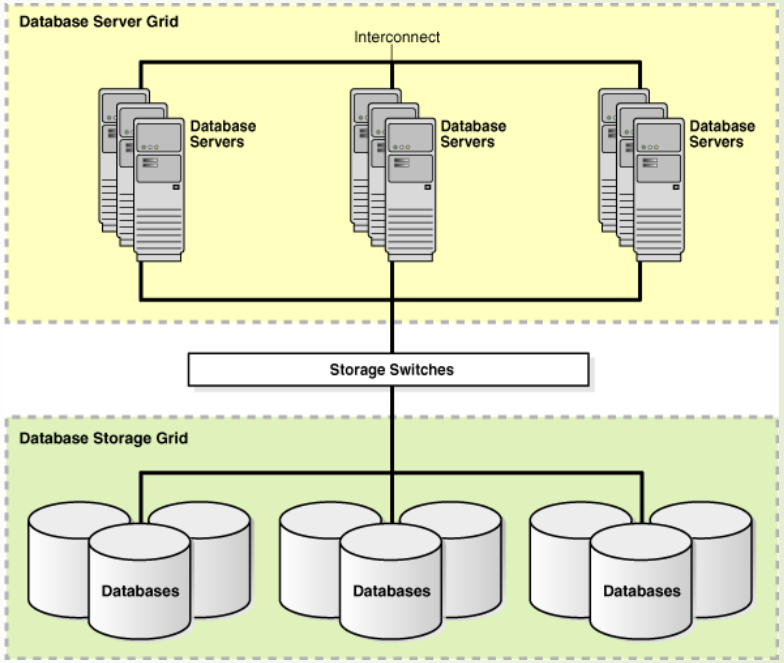
- **Data Query Language (DQL)**
  - **Select**
- **Data Manipulation Language (DML)**
  - **Insert / Update / Delete**
- **Data Definition Language (DDL)**
  - **Create / Alter / Drop**
- **Data Control Language (DCL)**
  - **Grant / Revoke**

Database Interface Languages

- Open Database Connectivity (ODBC)
  - Allows remote communication to DB
- Java Database Connectivity (JDBC)
  - Allows Java apps to communication to DB
- Extensible Markup Language (XML)
  - Standard for structuring data for use on the web
- Object Linking and Embedding (OLE)
  - Access to data no matter the location or format
- Active-X Data Objects (ADO)
  - Allows apps to access back-end DB systems

Database Replication and Shadowing

- Replication
  - Mirrors a live database allowing simultaneous reads and writes to multiple data bases
  - Has integrity issues (two phase commit)
- Shadowing
  - Mirrors all changes to the primary database
  - Clients do not access the shadow database
  - Serves as a live data backup



Database Vulnerabilities and Threats

- Aggregation
  - Combining information from sources to acquire knowledge when there is lack of clearance
- Inference: results of aggregation
- Bypass Attacks
  - Bypassing front-end controls
- Compromising Database Views
  - Lack of security labels / controls
- Denial of Service

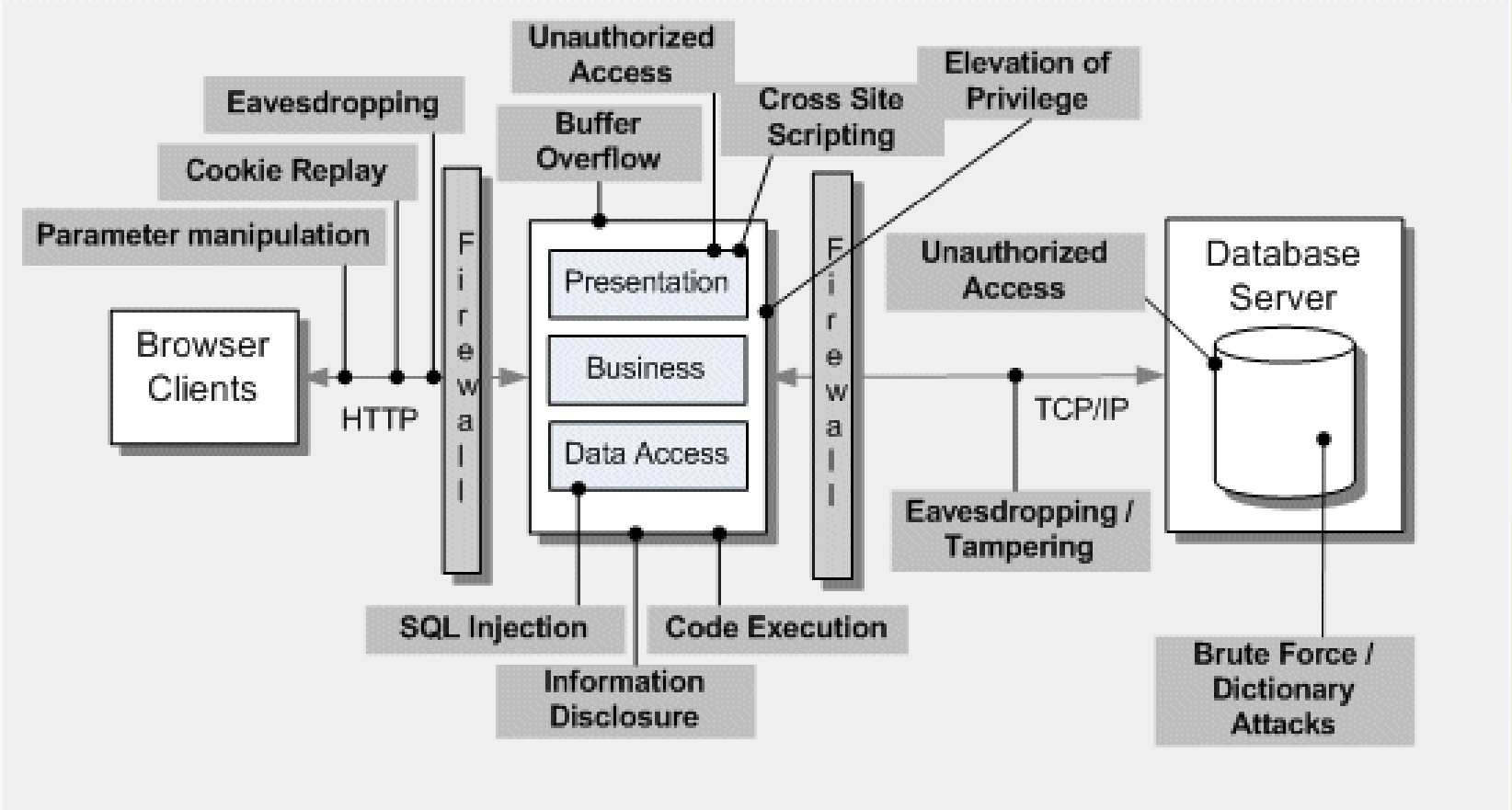
Database Vulnerabilities and Threats

- Concurrency: allows one change at a time
- Deadlocking: access to data at the same time, both are denied
- Data Contamination: data input errors
- Improper Modification of Information
- Data Mining

Database Vulnerabilities and Threats

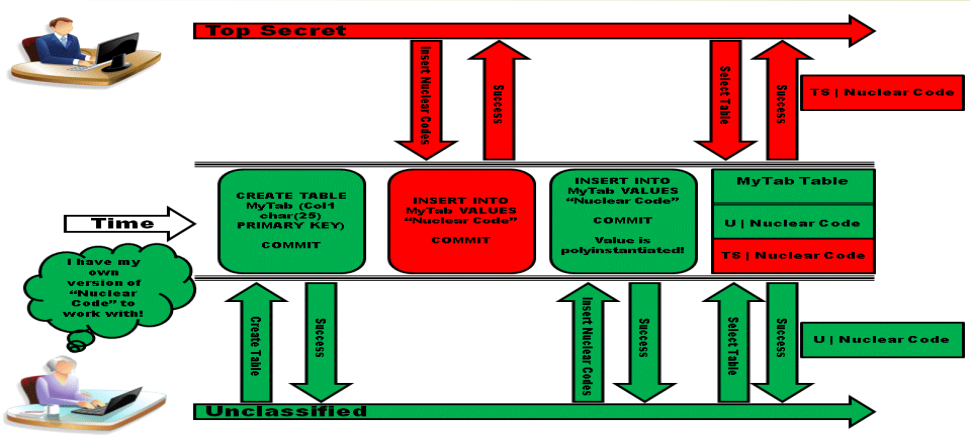
- Interception of Data
- Query Attacks
- Server/Database Access
- Time of Check/Time of Use
- Web Security
- Unauthorized Access
  - Unintentional release of info
  - Production data in DEVL or QA databases

Database Vulnerabilities and Threats



Polyinstantiation

- Polyinstantiation
  - Creating two versions of the same object
  - Versions are distinguished by security levels
  - Prevents Inference Attacks
  - Injects purturbation/distortion
  - Enables a relation to contain multiple rows with the same primary key



View Based Access Controls

- **Allows sensitive information to be hidden from unauthorized users**

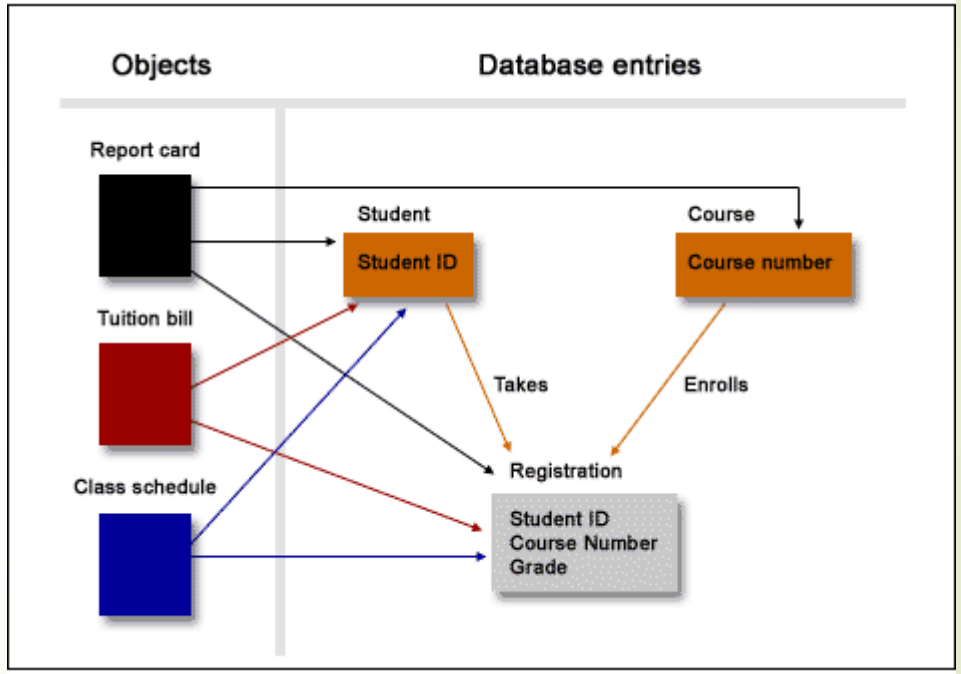
- **Ineffective, if the view based controls can be bypassed and if data can be manipulated directly**

Grant and Revoke Access Controls

- **Discretionary Access Control mechanisms**
- **A user could have permission to access a database and the authority to grant others to have access (Grant)**
- **If a user's permissions are revoked, all who have been granted similar permissions by that user are also revoked (Revoke)**
- **Users should not be able to pass grant authority to others**

Security for Object Oriented Databases

- Most security models are designed for relational databases
- Object Oriented Databases are more complex and therefore harder to secure
- When an instance of a class is created, it can automatically inherit the level of sensitivity of the superclass.



Metadata Controls

- Can manage restricted access to information
- Serves as a gatekeeper to filter access
- Metadata should be tightly bound to the data (do not move the data without the metadata)

Data Contamination Controls

- Input controls
  - Transaction counts, dollar counts, hash totals, error detection, error correction, resubmission, self-checking digits, control totals, and label processing
- Output controls
  - Reconciliation, physical handling procedures, authorization controls, verification, and audit trails

Online Transaction Processing (OLTP)

- Records all business transactions as they occur
- Acts as a monitoring system
- Detects when processes abort
- Restarts aborted processes
- Backs out failed transactions
- Allows distribution of multiple copies of application servers
- Performs dynamic load balancing

Additional Operations to Protect Data in a Database

- **Rollback**
  - **Ends current transactions**
  - **Cancels changes**
  - **Database returns to previous state**

- **Commit**
  - **Completes user transactions**
  - **Ensures partial changes do not take place**
  - **Two-Phase Commit**

Additional Operations to Protect Data in a Database

- Save Points
  - Ensures database can return to a point before a system crash
- Check Points
  - Saves data to a temporary file(when memory point reached)

Database Security Issues

- Content-Dependent access control
  - More sensitive the data, less access given
- Context-Dependent access control
  - Software understands which user actions are allowed
  - Based on state and sequence of request
- Cell Suppression
  - Hiding specific cells to avoid inference attacks

Knowledge Management

- Corporate/Organizational Memory
  - All the information an organization might possess
  - Grouped into a data warehouse
- Knowledge Discovery in Databases (KDD)
  - Mathematical, statistical, and visualization method of identifying valid and useful patterns in data
  - Mostly used via artificial intelligence

Expert Systems

- Rule Based (on If-Then Logic)
  - Uses artificial intelligence
- Built by Knowledge Engineers (analysts)
  - Emulates human logic to solve problems
  - A.k.a. Knowledge-based system
- Optical Character Recognition (OCR)
  - Used by scanners and other optical readers
- Components
  - Inference Engine
  - Knowledgebase

Neural Networks

- Based on the neural structure of the brain
- Programmed with the capability to decide and learn to improve its decision functionality
- Capability to “learn”
- Intelligent “Vacuum Cleaner”
- Voice recognition, weather prediction, etc.

Web Threats

- Web sites are the primary interface for e-Commerce
- Potential problems
  - Fraud
  - Theft

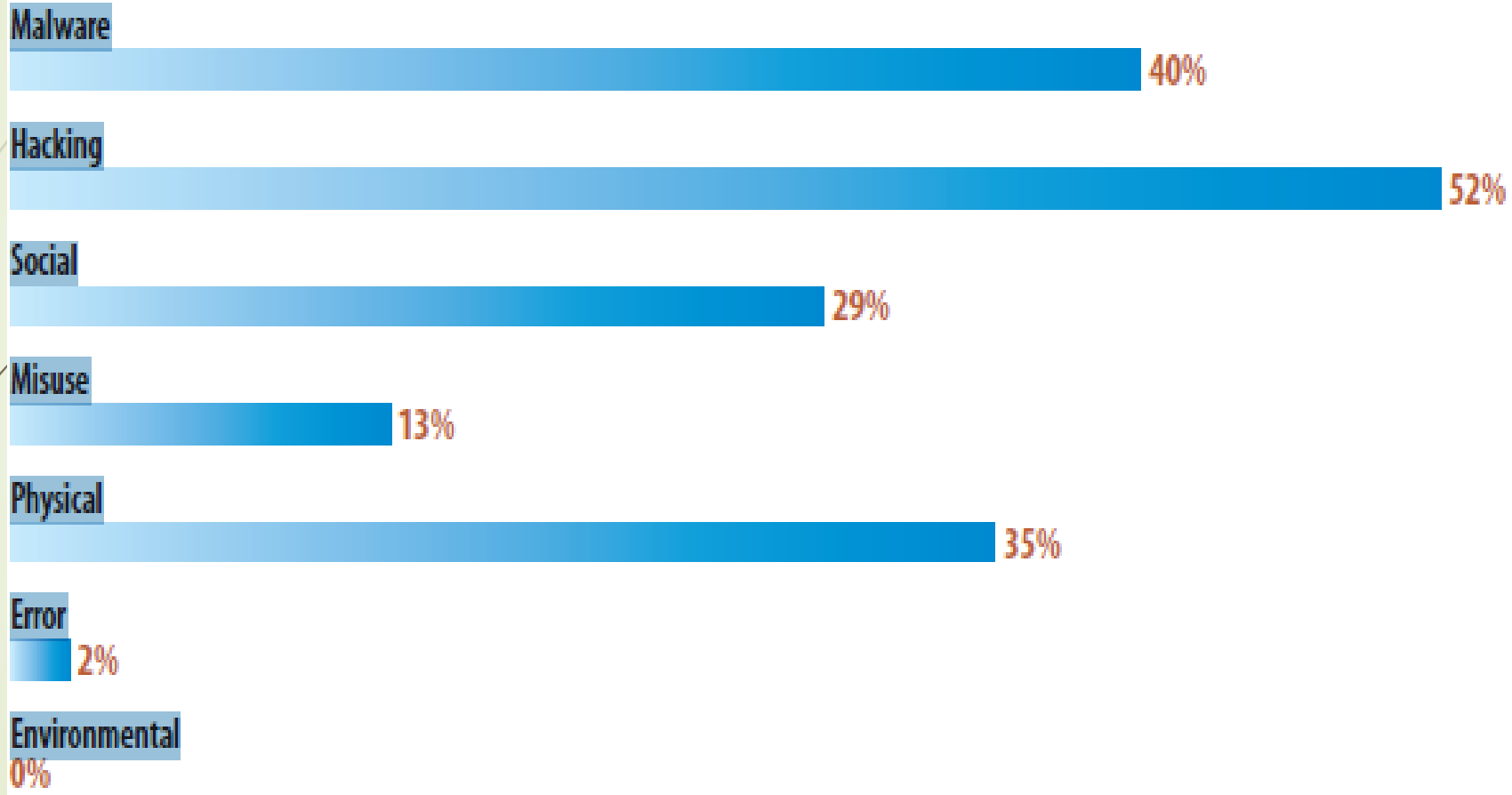
- Web sites can add a vector for intrusion into the private network
- Most attacks happen at the application level
- Web sites vulnerable due to accessibility

Top 10 Web Threats

- Drive By Downloads
- Click Jacking
- Plug-in and script enabled attacks
- Advanced Phishing Attacks
- Social Engineering Networks
- Watering Hole Attacks
- Third Party Web APPs
- Mobile Application Threats
- Malvertising
- P2P Dangers

Most Common Attack Methods

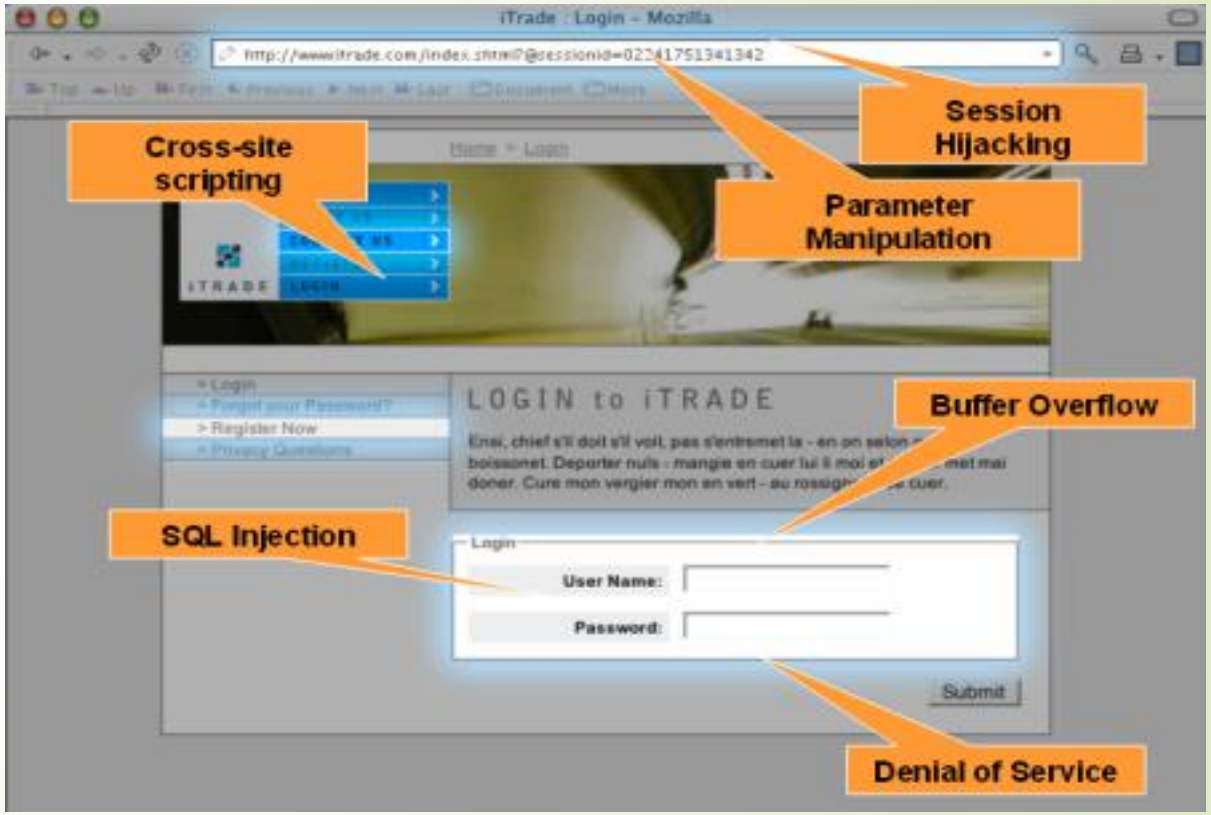
Malware and hacking are the most common methods used in data breaches. Many incidents require both malware and hacking in a one-two combo. Misuse primarily applies to insider incidents. Social engineering has quadrupled since 2011.



Data: Verizon 2013 Data Breach Investigations Report

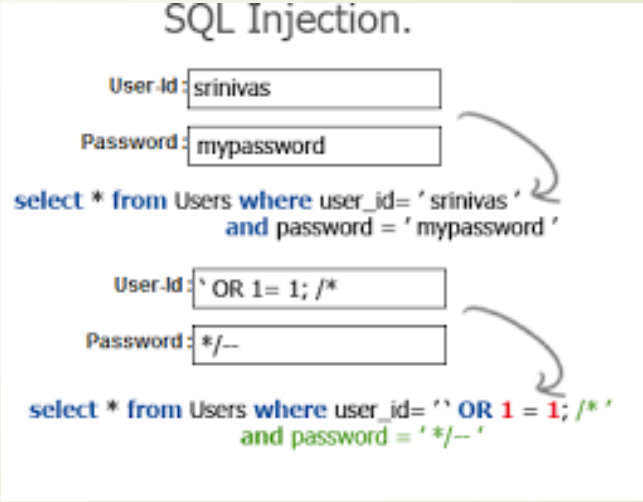
Web Input Validation

- Accepting Input:
  - Length
  - Type
  - Range of memory
- Prevents:
  - Buffer Overflows
  - SQL Injection
  - CGI Attacks



SQL Injection

- SQL Injection
  - Type of injection attack in which SQL commands are injected into data-plane input in order to effect predefined SQL commands. (OWASP)
  - Allows an attacker to query data from the database via the user interface
  - DoS is the most common SQL attack
  - (example)User ID = ‘ ‘ or 1=1;
    - Attempts to login as the database admin
  - Safeguards:
    - Input validation
    - Harden database
    - Parameterized queries
    - Stored procedures



Web Protection

- If you use cookies with programs, encrypt them
- Do not use sequential, calculable, or predictable cookies, session numbers, or URL data
- Validate all input and output
- Fail secure
- Do not cache secure pages
- Do not automatically trust data, regardless of source
- Audit

Current Software Environment

- Issues with Current Information Systems
  - Becoming more distributed
  - Increase in the use of open protocols, interfaces, and source code
  - Increased sharing of resources
  - Speed to Market
  - Malicious Code
  - Customer demand

Application Security Preview

- Software includes both operating systems and application software
- Application refers to agents, applets, databases, data warehouses, and knowledge-based systems
- Security must be considered in all aspects of the application lifecycle, such as:
  - Planning, Development, Implementation, Operation, and Maintenance

Programming

- Addressing Security at the Source
  - Past practices did not require security implementation
  - Security professionals are not software developers
  - Software developers are not security professionals
- Functionality versus Security
- Complexity of design

Application Development Methodology

- **Programming Language Evolution**
  1. **Machine**
  2. **Assembler**
  3. **High-level**
  4. **Very high level**
  5. **Artificial Intelligence**

- **Source code and Machine code**

- **Interpreters, Compilers, and Assemblers**

Top Down vs. Bottom Up Programming

- Top Down Programming
  - Starts with the highest level requirement and works down
  - Risks making incorrect assumptions about the lower level devices
  - Example: C programming

- Bottom Up Programming
  - Starts with low level technical details and works up
  - Risks wasting time developing features that will not be in the final product
  - Example: object oriented programming

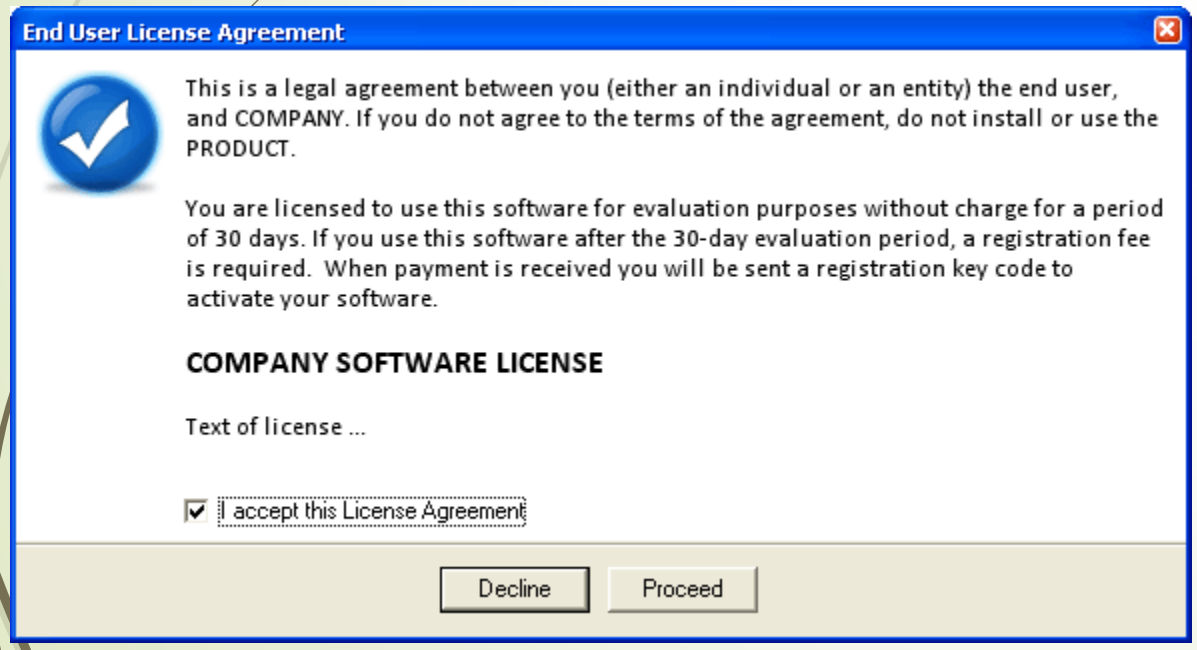
Open Source

- Code is freely available to those that chose to use it
- The more eyes on the code, the more likely the bugs will be discovered (Full Disclosure)
- There is no security through obscurity

Freeware/Shareware/Crippleware

- Freeware
  - Free of charge for use
- Shareware
  - Initially free but requires payment after a certain time frame
- Crippleware
  - Software has features turned off until the user pays the licensing fee

Licensing



- What does "FREE" really mean?
- End User Licensing Agreement (EULA)
- Open Source Licenses
  - GNU Public License (GPLv2, GPLv3)
  - Berkley Software Distribution License (BSD)
  - Apache Software Foundation License
  - Etc…

Copyleft vs. Copyright

- Copyleft
  - Copyleft attempts to negate copyright for the purposes of collaborative software development
  - Attempts to keep free software free
- Copyright
  - Source code is protected and only the author can decide to distribute code
  - Recipients may use the code but not alter it or create a derivative work

Software Escrow

- 3rd party stores archive of software
  - Party is neutral
  - Stores the source code
- Negotiated as contractual requirement with a software vendor
  - Protects the purchaser should the vendor go out of business

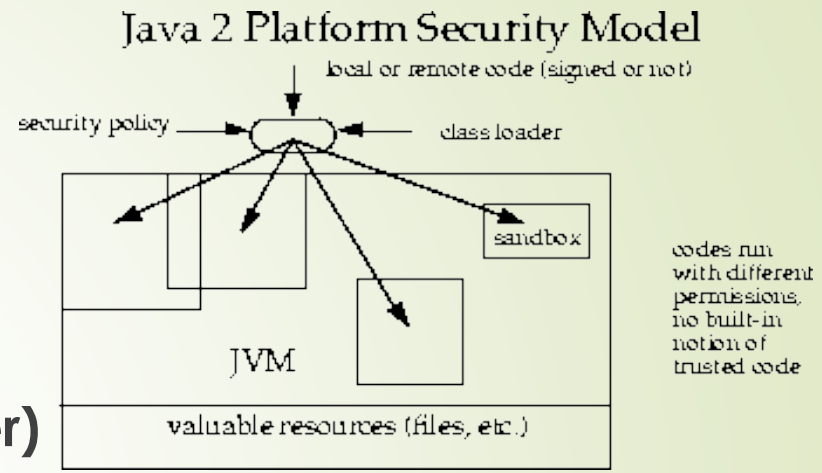
Disclosure

- Disclosure: The actions you take when you discover a flaw
- Full Disclosure: Release details of the flaw publically
  - Sometimes controversial and seen as unethical as it may aid the enemy by giving them knowledge they would not have otherwise possessed
- Responsible Disclosure: privately sharing the vulnerability info with the vendor until a patch is available.
  - Considered to be the ethical solution
  - Action may need to be taken if the vendor does not perform properly

Threats in the Software Environment Executable Content/Mobile Code

- **Software that is transmitted across the network to a local systems and executed on that system**
  - **Java Applets**
  - **Active X Components**
  - **Scripts / Plug-ins**

JAVA Security



- Java Applet
  - Client-side program that is platform independent
  - Runs inside another application (as in a web browser)
- Sandbox
  - A Virtual Machine (JVM) converts byte to machine code
  - Restricts the applets access to system resources
- Digital Signatures
  - Applets containing a digital signature can run outside of the virtual machine and be given access to system resources
  - Based on the trust conveyed by the certificate accompanying the digital signature

JAVA Security

- Java Steps
  - Programmer creates the code and compiles it with a Java compiler
  - Java compiler turns the source code into byte code
  - User downloads the Java Applet
  - The Java Virtual Machine converts the byte code into machine level code
  - Applet runs whenever called on

- Scripts and Plug-ins
  - Scripts run within the browser
  - Browser plug-ins increase the attack surface of the web browser (QuickTime/Adobe/Flash)

Mobile Code - ActiveX

- Controls used to interact with web pages
- Developed by Microsoft for Windows OS
- Downloaded to the user's hard drive
  - Greater access to system resources than Java
- PKI aware authenticode (code is digitally signed)
  - Relies on signature, certificates, and the user's awareness

Object Oriented Technology and Programming

- Message - how objects communicate
- Method - functionality an object can carry out
- Behavior - results or output of an object
- Classes - collection of common methods from a set of objects that defines their behavior
- Instance - examples of classes containing their method
- Delegation - forwarding of a request by an object to another object
- Cohesion and Coupling - (next slide)

Coupling and Cohesion

- Coupling
  - Level of interaction between objects
  - Low coupling means less interaction
  - Low coupling is easier to troubleshoot
- Cohesion
  - Degree to which an object depends on other objects
  - High cohesion: low dependence on other objects
  - High cohesion is easier to troubleshoot

Object Oriented Security

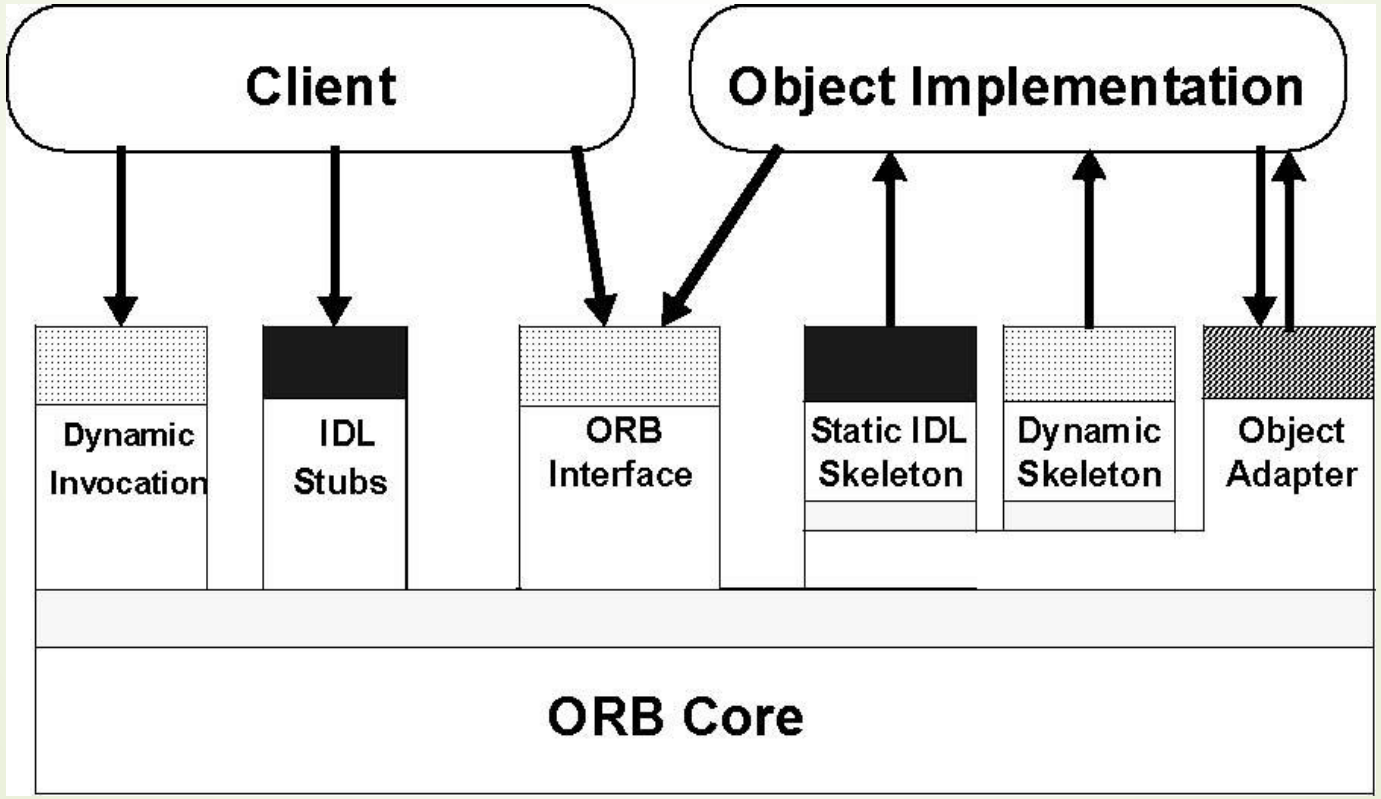
- Encapsulation (data hiding)
  - Protects private data from outside access
- Polymorphism
  - How different objects respond to the same command
- Inheritance (code reuse)
  - Occurrence when methods from a class (parent) are inherited by a subclass (child)

Distributed Object Oriented Systems

- Applications are broken into components
  - Components can exist in different locations

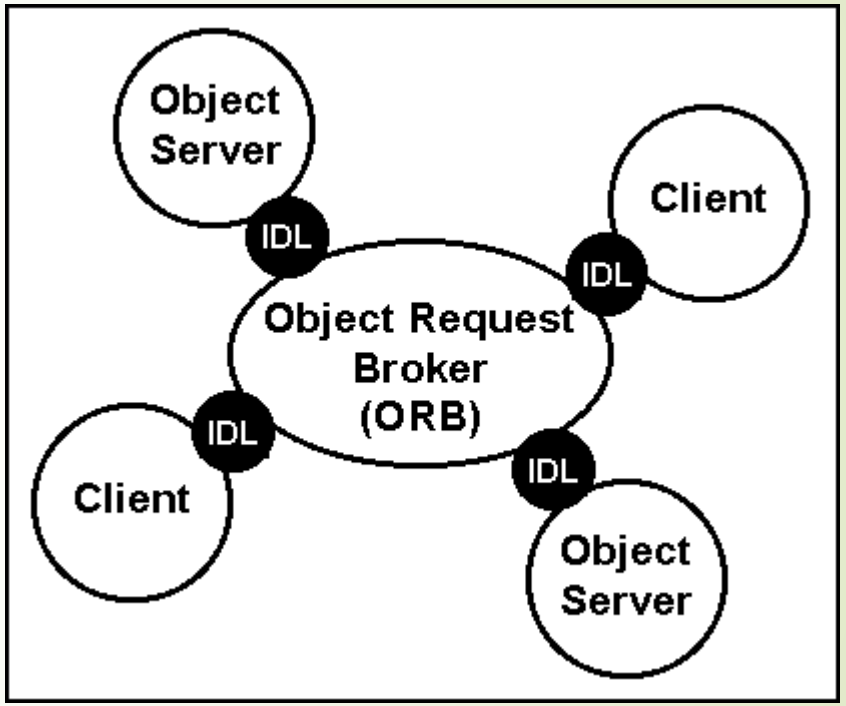
- Today's applications are designed on distributed objects such as:
  - Java Remote Method Invocation (JRMI) and Enterprise JavaBean (EJB)
  - Common Object Request Broker (CORBA)
  - Distributed Component Object Model (DCOM)

Common Object Request Broker Architecture (CORBA)



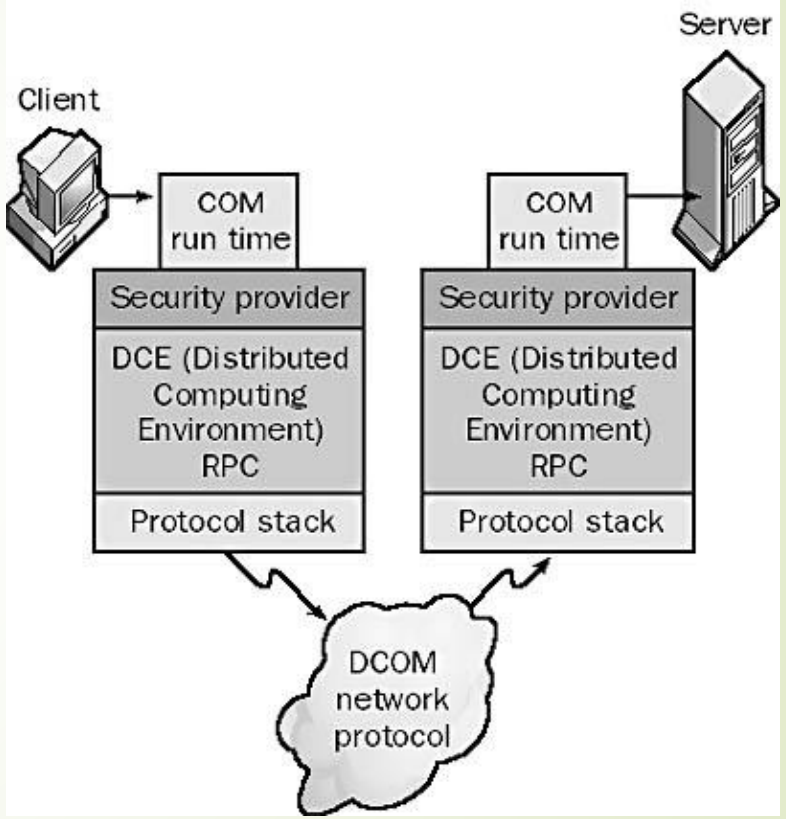
Object Request Brokers (ORB)

- Mechanisms that enable objects to communicate locally or remotely
- Object Management Group (OMG)
- Object Management Architecture (OMA)
- Interface Definition Language (IDL)
- ORB is Middleware
- Pipes



COM and DCOM

- Component Object Model (COM)
  - Microsoft's framework for developing and supporting components
  - COM objects allows other applications or components to access their features
- Distributed Component Object Model (DCOM)
  - Allows for applications to access objects on different parts of the network



COM and DCOM

- Application Programming Interface
  - Interface between an application process and the TCP/IP protocol stack
- Globally Unique Identifier (GUID)
  - Application identifier which provides a unique reference number
  - Used in the registry to identify COM DLLs
- Object Linking and Embedding (OLE)
  - Allows embedding and linking to objects developed by Microsoft

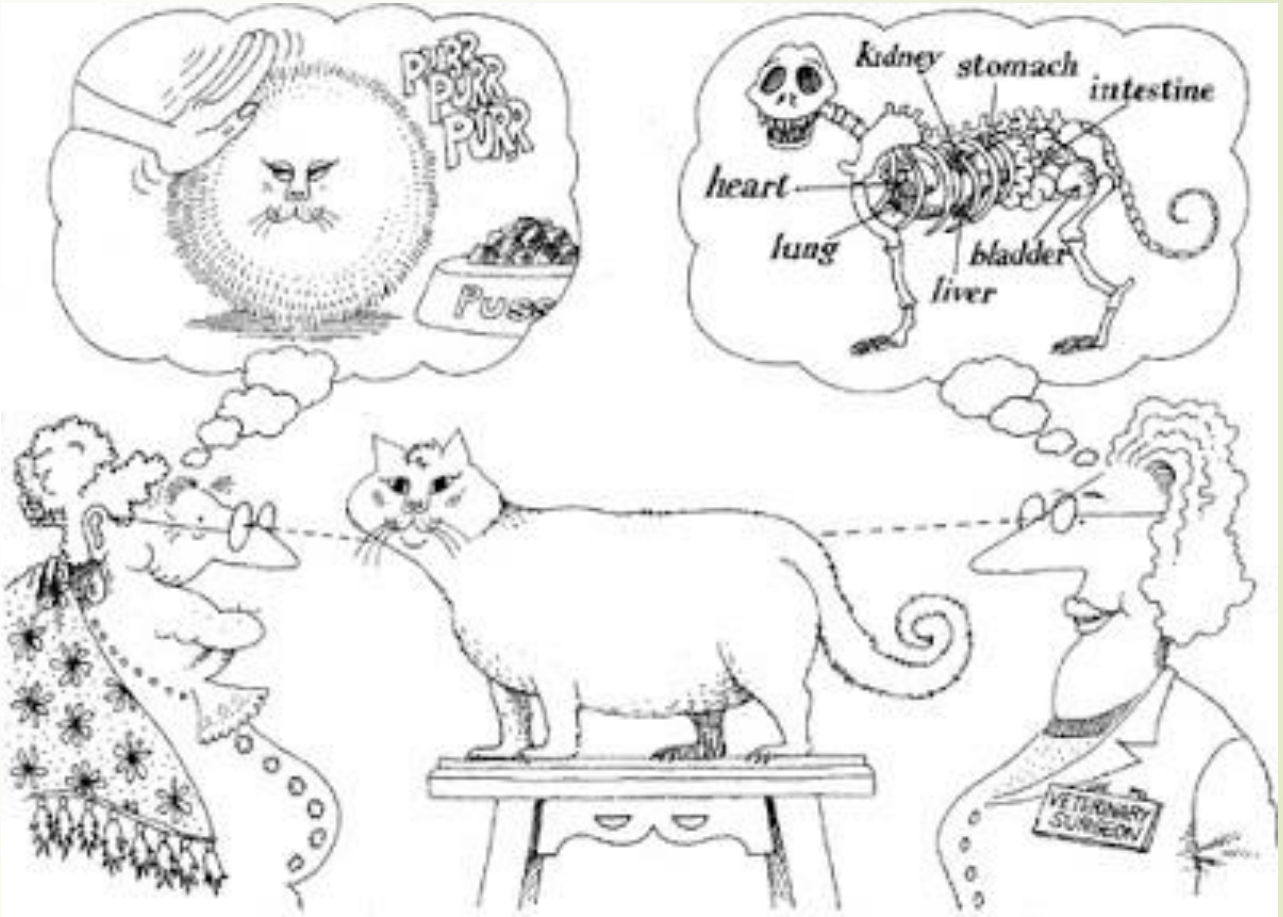
IPC and DICP

- Inter-Process Communication (IPC)
  - Mechanisms that facilitate communication and data exchange between processes or threads (child processes)

- Distributed Inter-Process Communication (DIPC)
  - Software-only solution for distributed data exchange and programming under Linux
  - Enables programmers to write distributed software without the need to know about network programming

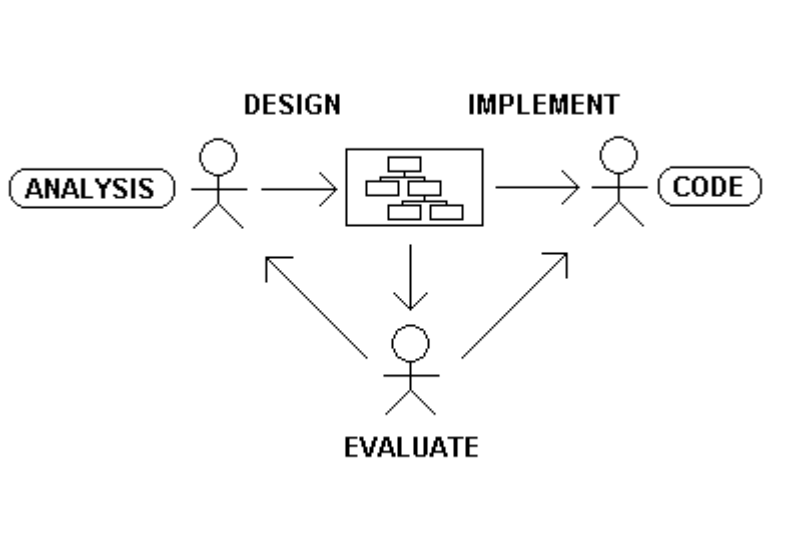
Object Oriented Analysis (OOA)

- Seeks to understand the problem
- Identifies all objects and their interaction
- Uses Unified Modeling Language (UML)



Object Oriented Design (OOD)

- Sometimes combined with Object Oriented Analysis (OOAD)
- Develops the solution based on the analysis
- Uses Unified Modeling Language (UML)

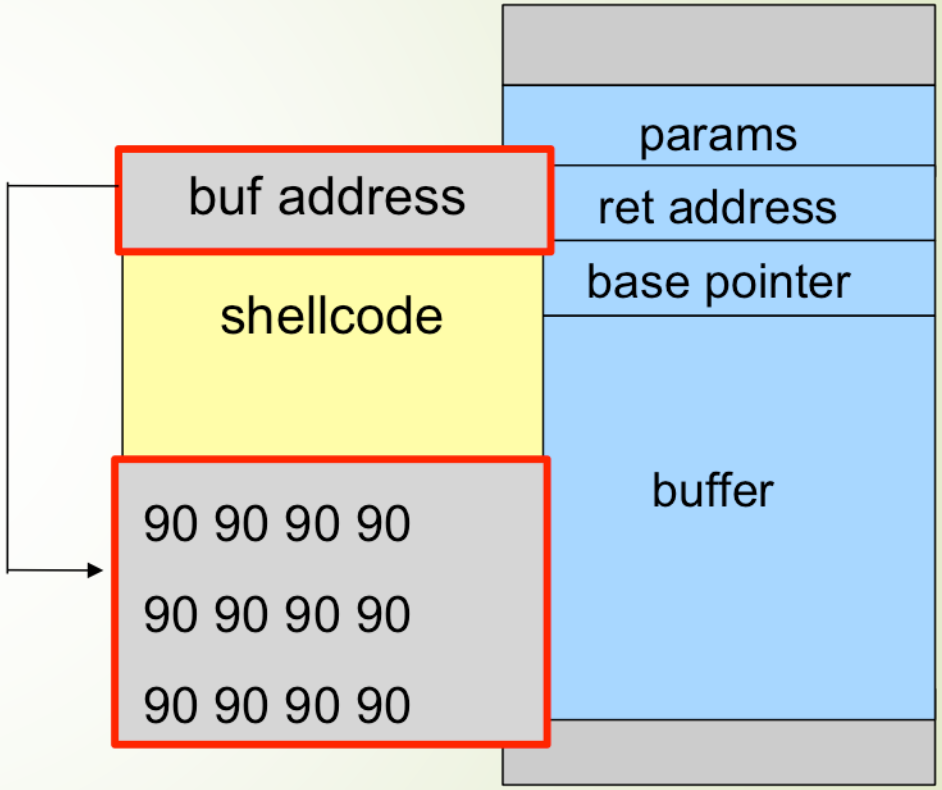


Threats in the Software Environment Buffer Overflow

- One of the oldest and most common of software problems
- Caused when a program fills up its buffer of memory with more data than it can hold
- Can lead to the insertion of malicious code used to gain administrative access
- Caused by insufficient bounds checking (data length, type, format)

Buffer Overflows

- Caused by ineffective parameter checking
  - Implemented by the programmer
- Perform bounds enforcement and error checking
  - Check data length/type
- Hardware states and hardware controls make buffer overflows impossible
- Patch or upgrade



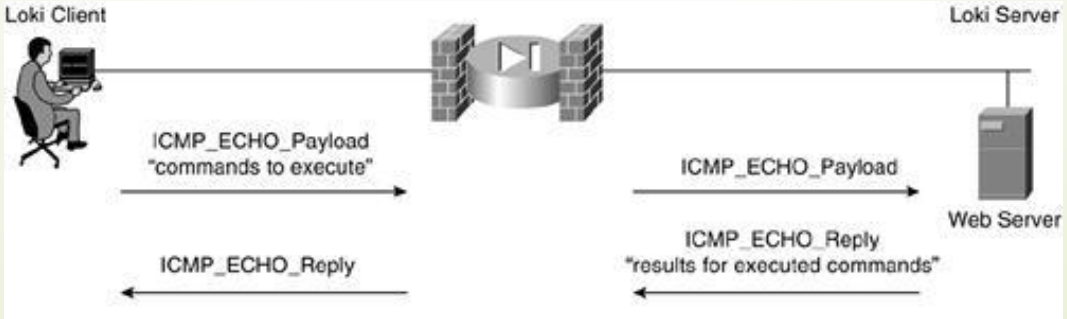
Threats in the Software Environment Citizen Programmers

- Anyone can learn a programming language and become a programmer
- Not trained in or bound by system development practices
  - No proper application design
  - No change control
  - No support for the application
- Software creations are often developed chaotically and lack security

Covert Channels

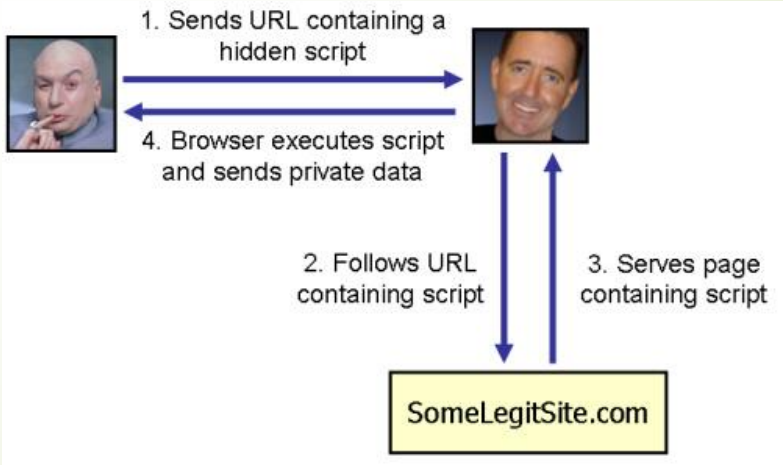
- Communication channel allowing two cooperating processes to transfer information in such a way that it violates the security policy

- Two commonly defined types
  - Storage: One process writes data to a storage location and another process directly or indirectly reads it
  - Timing: One process relays information to another by modulating its use of system resources



Software Vulnerabilities

- Hard-coded Credentials (backdoors)
- Buffer Overflow
- SQL Injection
- Directory Path Traversal
- PHP Remote File Inclusion
- Cross-site Scripting & Cross-site Request Forgery
- Privilege Escalation
- Backdoors

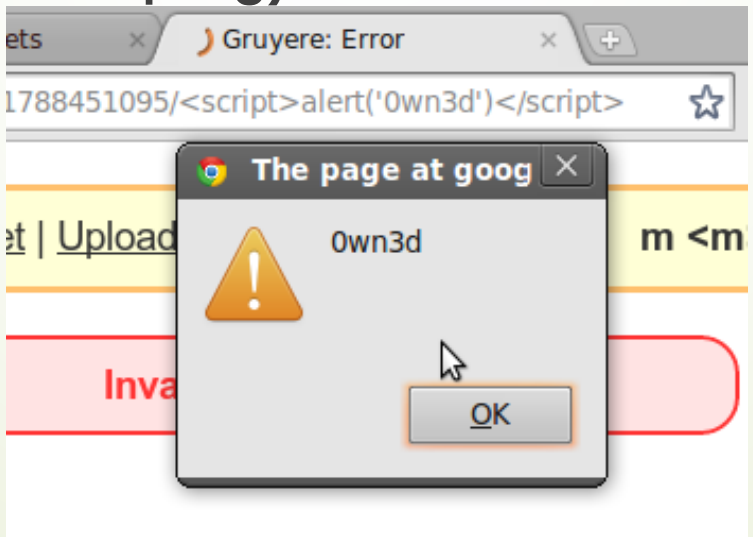


Threats in the Software Environment Malicious Software (Malware)

- Virus
- Trojan Horse
- Logic bomb
- Worm
- Ad/Spy ware

Malformed Input Attacks

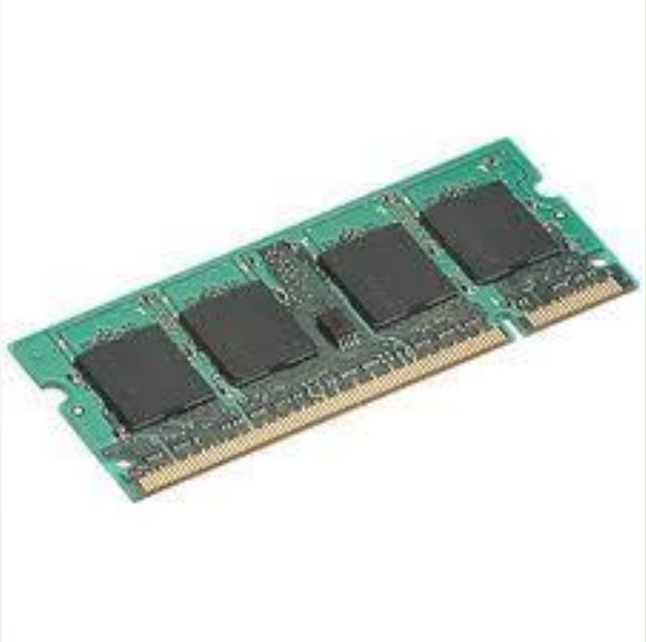
- Attacks employing specially crafted user input
- Examples:
  - Unicode format for a browser URL that bypasses firewall rule sets
  - Structured Query Language (SQL) queries in the browser URL box (cross-site scripting)



Threats in the Software Environment Memory Reuse (Object Reuse)

- Memory Management involves
  - Allocating memory space to one process
  - Re-allocating it upon process completion
  - Then re-allocating it to a new process

- Problem
  - Residual information



Threats in the Software Environment Social Engineering

- Sometimes referred to as "people hacking"
- Has the ability to circumvent access controls
- Malicious software will often contain a fraudulent component in an attempt to get a user to run the program

Threats in the Software Environment Time of Check/Time of Use (TOC/TOU)

- A form of asynchronous attack (time)
- Occurs when a program checks access permission too far in advance of a resource request
- The attack gets in between steps and makes modifications
- How to Mitigate:
  - Have software lock the items it will use while carrying out its checking tasks

Threats in the Software Environment Between the Lines Attack

- **Communication lines are tapped into and data is falsely inserted**
- **Mitigate by physically securing lines and training users to not leave lines open when not in use**

Threats in the Software Environment Trapdoor/Backdoor

- A.K.A. Maintenance or Programming Hook
- Software entry point that is inserted by the programmer
- Allows developers to bypass normal access restrictions

Malicious Code - Malware

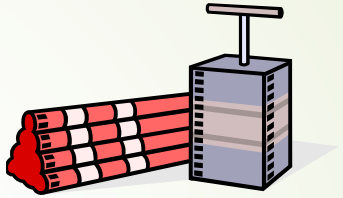
- Viruses
  - Stealth
    - Hides by tampering with the OS to fool antivirus software
    - Encryption/Compression will help hide the virus
  - Polymorphic
    - Mutates by modifying its own code as it travels from system to system, while still keeping the original algorithm intact
    - Makes pattern recognition hard
  - Macro Virus

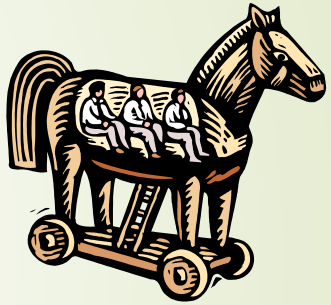
Malicious Code - Malware

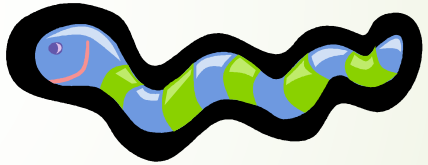
- Viruses
  - Oligomorphic
    - Code similar to polymorphic, but has a decryptor that does not show up on signature list
  - Metamorphic
    - Reprograms itself; carries various versions of itself
    - Translates itself into temporary representations and then back to normal code
    - Capable of infecting more than one OS
  - Zoo Viruses
    - Laboratory viruses not found in the wild

Malicious Code - Malware

- Antivirus Mechanisms
  - Signature Based Detection
  - Heuristic Based Detection
- Hoaxes
- Logic Bomb
- Trojan Horse
- Worm
- Agents/Bots
- Spyware
- Packers





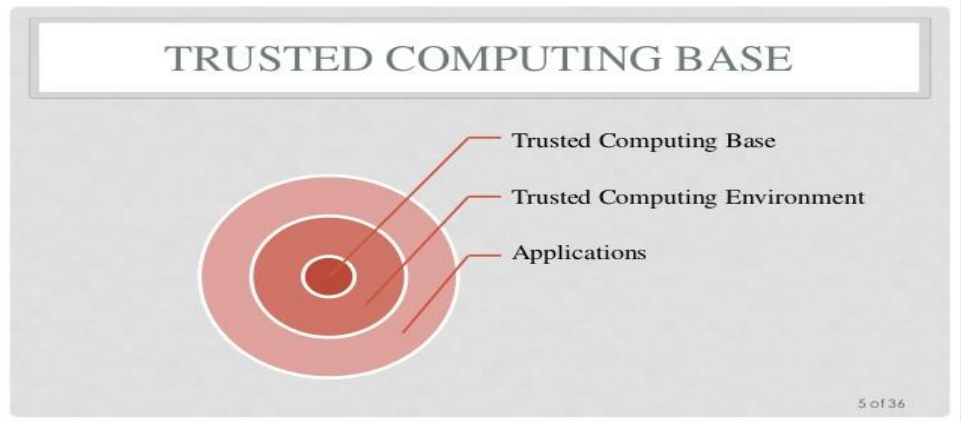


Rootkits

- 4 generations of root kits
- An undetected assembly or collection of programs and code that allows constant presence on a computer or automated information system
- A collection of tools, binaries, scripts, configuration files that allow intruders to conceal their activity on a computer so that they can covertly monitor and control the system for an extended period
- Exist to provide sustained covert access to a machine so that the machine can be remotely controlled and monitored in a manner that is extremely difficult to detect

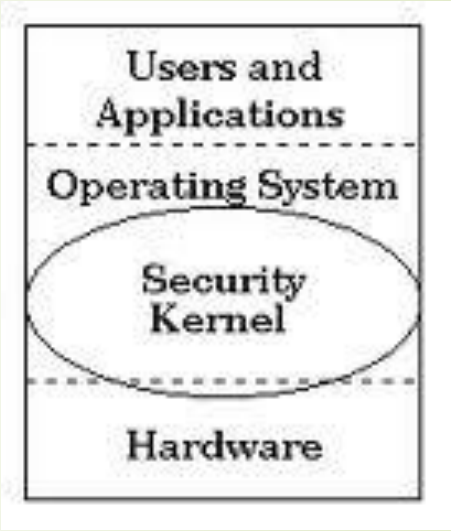
Trusted Computing Base (TCB)

- All hardware, firmware, and software components that are critical to a computer's security
- All code that runs in the privileged mode of the underlying processor is part of the TCB
- In a Linux/Unix system, any daemon running as root would be part of the TCB



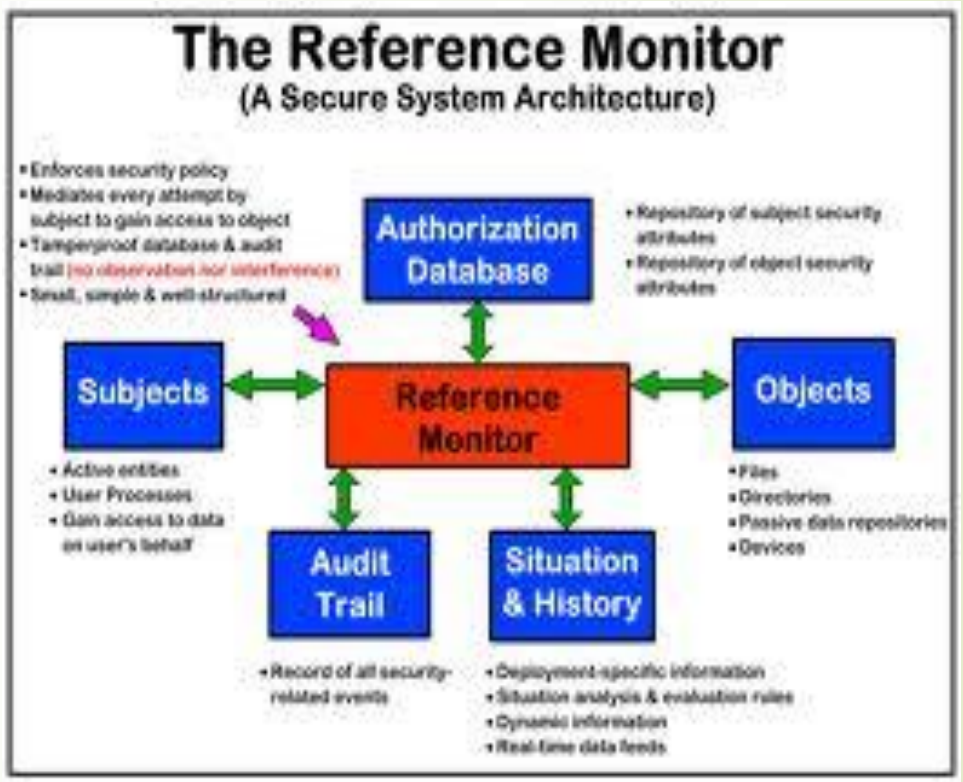
Security Kernels

- The hardware/software component that implements the concept of the reference monitor
- Security kernel requirements:
  - Completeness: All access to information must go through the kernel
  - Isolation: The kernel must be protected from any type of unauthorized access or modification
  - Verifiable: Must be proven to meet design specifications
- Reference Monitor performs security checks
  - Mediates all access between subjects and objects
  - Always enabled-can not be bypassed



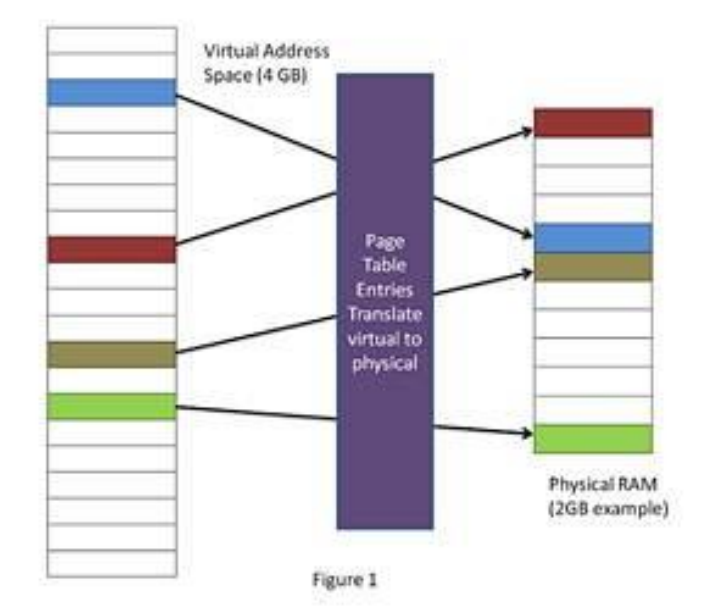
Reference Monitors

- Validates access to resources
  - Evaluates the subject's security clearance to the object's security label
  - Implemented and enforced by the Security Kernel



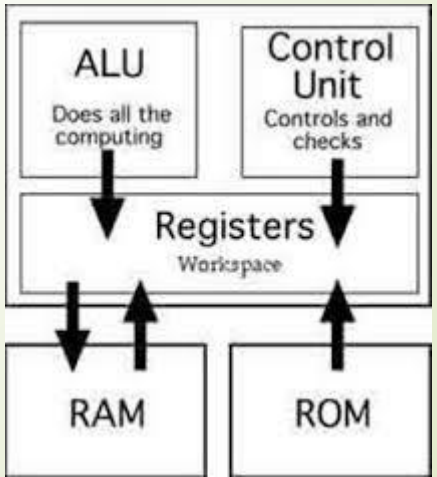
Memory Manager

- Operating system function that keeps track of how different types of memory are used
- Allocates/de-allocates memory, enforces access control (isolation), and manages swapping memory from RAM to hard drive
- Five responsibilities
  - Relocation
  - Protection
  - Sharing
  - Logical organization
  - Physical organization



Registers

- Base and Limit Registers
  - Base identifies the beginning address assigned to a process
  - Limit identifies the ending address
  - Threads will reference addresses and the CPU verifies the request is within the confines of the memory space allotted



Memory Protection Methods

- Kernel mode and user mode are kept separate
- Each process has a separate, private address space
  - Address Space Layout Randomization (ASLR)
- Hardware or software memory protection
  - Data Execution Prevention (DEP)
- Access control lists to protect shared memory objects

Baselining

- A captured point in time where current system security configuration is understood
- Creates a common security configuration
- Helpful when responding to security incidents
- Makes recovery of systems easier
- Effective method of providing a required level of protection across a broad area

Security of Application Programming Interfaces (API)

- Connections that allow devices to speak to each other
- Unknown and unseen force of the Internet
- When GPS device sends info to a website it uses an API
- Data governance
  - Structured and controlled development and deployment of APIs that will be used to manage and secure all data exchanges

Representational State Transfer (REST) API

- Simple way to organize interactions between independent systems
- REST allows you to interact with minimal overhead with clients as diverse as mobile phones and other websites
- Inspired by HTTP. As a result, REST can be used wherever HTTP can
- Often uses JavaScript Object Notation (JSON)
- Not a web standard, (Example):

http://www.vikings.com/team/players/12345

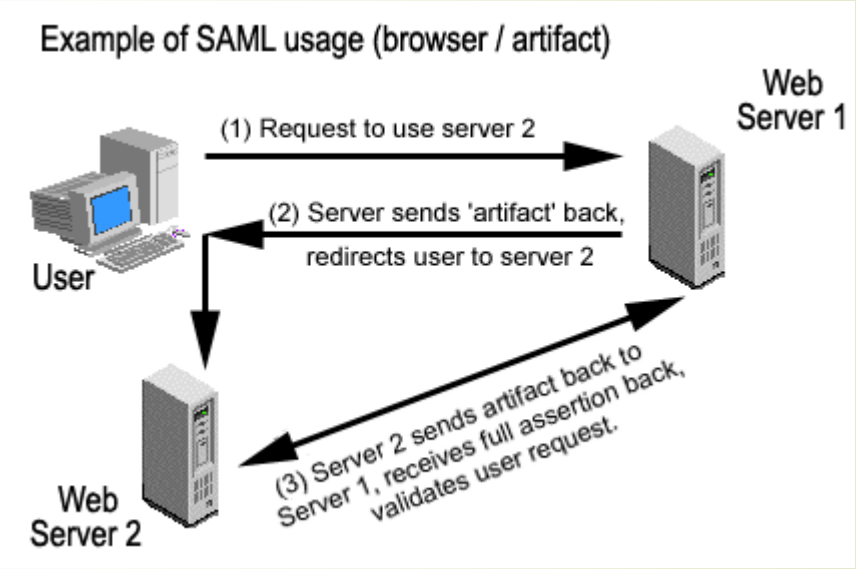
JavaScript Object Notation (JSON)

- JSON: JavaScript Object Notation.
- JSON is a syntax for storing and exchanging data.
- JSON is an easier to use alternative to XML
- (EXAMPLE)

```
{"employees":[
    {"firstName":"John", "lastName":"Doe"},
    {"firstName":"Anna", "lastName":"Smith"},
    {"firstName":"Peter", "lastName":"Jones"}
  ]}
```

XML/SAML

- XML (Extensible Markup Language)
  - Standard for encoding documents and data
  - More versatile than HTML
  - Not restricted for web use only
- SAML (Security Assertion Markup Language)
  - Security information exchange framework
  - Part of a plan to make web access single sign on (SSO)
  - Used by some forms of SSO



Security Assertion Markup Language (SAML)

- Advantages
  - Platform Neutrality
  - Loose Coupling of Directories
    - No synchronization
  - Improved Online Experience for End Users
    - Enables single-sign-on
  - Reduced Administrative Costs for Service Providers
    - Reduced account maintenance via SSO
  - Risk Transference
    - Pushes responsibility for identity management to identity provider

Service Oriented Architecture (SOA)

Web Services Security

- Web Services Security (WS-Security, WSS) is an extension to Simple Object Access Protocol (SOAP) to apply security to Web services.
- The protocol specifies how integrity and confidentiality can be enforced on messages
  - Allows the communication of various security token formats, such as Security Assertion Markup Language (SAML), Kerberos, and X.509.
- Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.

Bayesian Filtering

- Commonly used to identify SPAM
- Statistical probability filtering (mathematical probability)

Genetic Algorithms and Programming

- Programs evolve to solve a problem
  - Create entire software programs (LISP source code)
  - Shorter pieces of code (stings called chromosomes)
- Create random programs and assign them tasks of solving a problem
- Darwinian in nature (survival of the fittest) as programs swap code and form new code
- Search algorithms are an example

Three paths to authenticating APIs

- Basic Authentication with TLS (basic Username/password)
- Oauth1.oa
  - Most secure
  - Uses cryptographic signature (HMAC-SHA1) values that combine token secret, nonce and other request based information.
  - Token is never passed over the wire (requires no SSL)
- Oauth2
  - Does not use signatures; uses TLS
  - Has less coding libraries than Oauth1.oa
- Key Management Interoperability Protocol (KMIP) and HTTP Digest are also possible solutions

Certification/Accreditation

- Four Step Process
  - Initiation Phase
  - Security Certification Phase
  - Security Accreditation Phase
  - Continuous Monitoring Phase

Risk Management Framework

- Has been formulated from the traditional certification and accreditation process
- Six Step Risk Management Framework
  - Promotes near real time risk management and implements robust continuous monitoring
  - Encourages automation in support of informed decisions
  - Integrates information security into the architecture and SDLC
  - Provides emphasis on selection, implementation, assessment and monitoring of security controls
  - Links risk management processes at the information system level to risk management processes
  - Establishes responsibility and accountability for security controls

Risk Analysis and Mitigation

- Once a risk has been documented:
  - Identify the mitigation steps that can be taken to lessen the probability of the event occurring
  - Create a contingency plan that goes into effect either prior to or when the event occurs
- Evaluate the probability of each risk against the mitigation strategy cost before deciding to implement a contingency plan
  - Contingency plans implemented prior to an event are pre-emptive actions intended to reduce or remove the risk.
  - Contingency plans implemented after an event only lessen the impact

Risk Analysis and Mitigation Strategy

- Integrate into the overall SDLC and change management process
- Use standardized methods of reporting risk
  - Qualitative versus quantitative versus hybrid
- Track and manage discovered weaknesses
- Document risk decisions to aid due diligence

Corrective Actions

- Software products have numerous security weaknesses that are only identified after they are fielded
  - Patch management
    - Have a backup, backout plan, target non critical systems first
  - Change management
  - Vulnerability testing

Testing and Verification

- Independent Verification and Validation (IV&V) teams work to determine if security issues are truly resolved
- Code signing certificates help protect users from downloading compromised code.
- Code Signing:
  - Security technique to ensure code integrity
  - Identify who developed the code
  - Determine if code is trustworthy

Code Signature

- Three parts:
  - A seal which is a collection of various hashes from various parts of the code
  - A digital signature which signs the seal and guarantees its integrity
  - A unique identifier which is used to identify the code to the group or category it belongs.

- Signing does not:
  - Guarantee code to be free of compromise
  - Guarantee that the app will not load altered or unstable code
  - Provide protection under Digital Rights Management

At Issue

- Increases in business and mission risk is attributable to software
- Exploitable software is vulnerable to attack
- Software vulnerabilities jeopardize:
  - Intellectual property
  - Consumer trust
  - Business operations and services
  - Critical infrastructure
  - Process control systems
  - Commercial software products

Software Assurance (SwA)

- Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that it functions in the intended manner

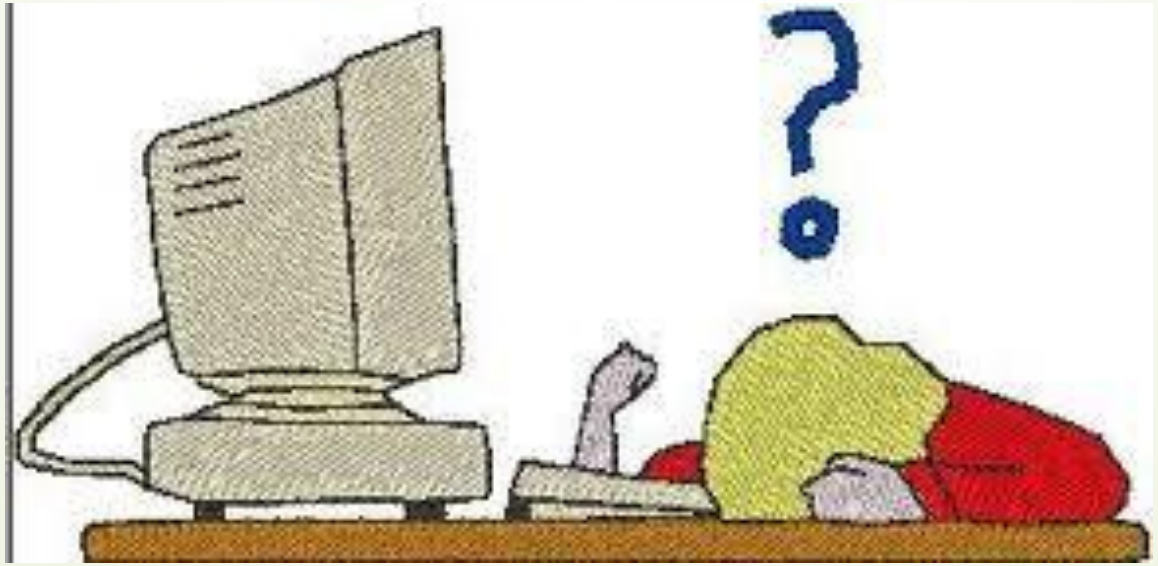
- SwA needs to be verified in the major phases of the generic acquisition process
  - Planning phase
  - Monitoring and acceptance phase
  - Follow-on

Software Assurance (SwA)

- Planning Phase
  - Determine needs
  - Develop requirements
  - Create an acquisition strategy that includes risk identification
  - Develop evaluation criteria

- Monitoring and Acceptance Phase
  - Establish a contract work schedule
  - Implement change control procedures
  - Implement a plan for review and acceptance of deliverables

Software Assurance (SwA)

- **Follow-On**
  - **Sustainment (includes risk management, assurance case management, and change management)**
  - **Disposal or decommissioning**
  - **Risk management**

Questions?