# INFOSYS 341 EXAM NOTES

# SESSION 2: Cryptography

**Basic definitions**

* Cryptography: process of making and using codes to secure transmission of information
* Encryption: converting original message into a form unreadable by authorized individuals
* Decryption: The process of converting the ciphertext message back into plaintext
* Cryptanalysis: Process of obtaining original message from encrypted message without knowing algorithms
* Cryptology: science of encryption; combines cryptography and cryptanalysis.
* Key space: the entire range of values that can be sued to construct and individual key.

**Foundations of Cryptology**

* Cryptology is made up of both cryptography and cryptanalysis. The first, cryptography, is the actual securing, control, and identification of digital data. The second, cryptanalysis, is made up of all the attempts one might develop to undermine, circumvent, and/or break what the first part, cryptography, is attempting to accomplish.

**Cipher methods**

* Plaintext can be encrypted through bit stream or block cipher method
* Bit stream: each plaintext bit transformed into cipher bit **one bit at a time**
* Block cipher: message divided into **blocks** and each is transformed into **encrypted block of cipher bits** using **algorithm and key**.

**Substitution Cipher**

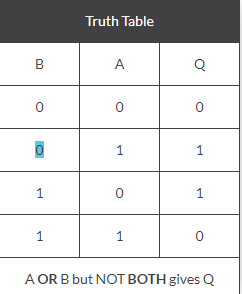
* Substitute one value for another
* Monoalphabetic substitution: uses only one alphabet
* Polyalphabetic substitution: more advanced; uses two or more alphabets
* Vigenere cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets.

**Vigenere Cipher**

* A method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword.

**Transposition Cipher**

* Easy to understand, but if properly used, produces ciphertext that is difficult to decipher.
* Rearranges values within a block to create ciphertext.
* Can be done at the bit level or at the byte level
* To make the encryption even stronger, the keys and block sizes can be done much larger.

**Exclusive OR (XOR)**

* Function of Boolean algebra; two bits are compared
  + If two bits are identical, result is binary 0
  + If two bits not identical, result is binary 1.
* A very simple symmetric cipher that is used in many applications where security is not a defined requirement.

**Vernam Cipher**

* Developed at AT&T
* Uses set of characters once per encryption process
* To perform:
  + The pad values are added to numeric values that represent the plaintext that needs to be encrypted
  + Each character of the plaintext is turned into a number and a pad value for that position is added
  + The resulting sum for that character is then converted back to a ciphertext letter for transmission
  + If the sum of the two values exceeds 26, then 26 is subtracted from the total.

**Book Cipher**

* This ciphertext consists of a list of codes:
  + Representing page number
  + Line number
  + Word number of the plaintext word.
* The algorithm is the mechanical process of looking up the references from the cipher text
* Converting each reference to a word by using the ciphertext’s value and the key (the book).

**Hash Functions**

* Mathematic algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm message identity and integrity.
* Hash algorithms: publicly known functions that create hash values
* Use of keys not required
  + Message authentication code (MAC), however, may be attached to a message
* Used in password verification systems to confirm identity of user.

**Cryptographic Algorithms**

* Often grouped into two broad categories, symmetric and asymmetric
  + Today’s popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms.
  + Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations.

**Symmetric Encryption**

* Uses same “secret key” to encipher and decipher message
  + Encryption methods can be extremely efficient, requiring minimal processing
  + Both sender and receiver must possess encryption key
  + If either copy of key is compromised, an intermediate can decrypt and read messages.
* Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that encryption and decryption are executed quickly, even by small computers.
* If the key falls into the wrong hands, message can be decrypted by others and the sender and intended received may not know a message was intercepted.

**Symmetric Encryption (Cont’d)**

* Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
  + 64-bit block size; 56-bit key
  + Adopted by NIST in 1976 as federal standard for encrypting non-classified information
* Triple DES(3DES): created to provide security far beyond DES
* Advanced encryption standard (AES): developed to replace both DES and 3DES. Used within the U.S government to protect information in federal agencies that are not part of the national defence.

**Asymmetric Encryption**

* Also, known as public-key encryption
* Can be inefficient if there are multiple parties involved.
* Uses two different but related keys
  + Either key can encrypt or decrypt message
  + If key A encrypts message, only key B can decrypt
  + Highest value when one key serves as private key and the other serves as public key
* RSA algorithm – was the first public-key encryption algorithm developed and published for commercial use. It is very popular and has been embedded in both Microsoft and Netscape web browsers to provide security for e-commerce applications.

**Encryption Key size**

* When using ciphers, size of cryptovariable or key is very important.
* Important for users to decide on the size of the cryptovariable or key
  + Strength of many encryption applications and cryptosystems is measured by key size.
  + The length of the key increases the number of random guesses that have to be made in order to break the code
  + Creating larger universe of possibilities increases the time requires to make guesses.

**Cryptographic tools**

* Potential areas of use include:
  + Ability to conceal the contents of sensitive messages
  + Verify the contents of messages and the identities of their senders
* Tools must embody cryptographic capabilities so that they can be applied to the everyday world of computing.

**Public-Key Infrastructure (PKI)**

* Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely.
* PKI systems based on public-key cryptosystems
* PKI protects information assets in several ways:
  + Authentication
  + Integrity
  + Privacy
  + Authorization
  + Nonrepudiation

**Public-Key Infrastructure (PKI) (cont’d)**

* Typical PKI solution protects the transmission and reception of secure information by integrating:
  + A certificate authority (CA)
  + A registration authority(RA)
  + Certificate directories
  + Management protocols
  + Policies and procedures

**Digital signatures**

* Created in response to rising need to verify information transferred using electronic systems
* Asymmetric encryption processes used to create digital signatures
* Nonrepudiation: the process that verifies the message was sent by the sender and thus cannot by refuted
* Digital signature standard(DSS)

**Digital Certificates**

* Electronic document containing key value and identifying information about entity that controls key
* Digital signature attached to certificates container file to certify file is from entity it claims to be from.
* Different client-server applications use different types of digital certificates to accomplish their assigned functions
* Distinguished name (DN): uniquely identifies a certificate entity

**Hybrid Cryptography Systems**

* Except with digital certificates, pure asymmetric key encryption not widely used
* Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
* Diffie-Hellman Key exchange method:
  + Most common hybrid system
  + Provided foundation for subsequent developments in public-key encryption
  + Facilitates exchanging privates using public-key encryption.

**Steganography**

* Process of hiding information
* Using the least significant bit
  + Every byte is made up of 8 bits
  + However not all of these 8 bits are necessary to define if a pixel of an image is red or white. This is the perfect spot to hide secret data since it doesn’t add any size to the file and it doesn’t alter the file itself.

**Protocols for secure communications**

* Much of the software currently used to protect the confidentially of information are not true cryptosystems.
* The lack of threats in the environment in which the internet was launched allowed it to grow rapidly.

**Securing Internet communication with S-HTTP and SSL**

* Secure socket layer (SSL): uses public key encryption to secure channel over public internet
* Secure Hypertext Transfer protocol (S-HTTP): extended version of hypertext transfer protocol: provides for encryption of individual messages between client and server across internet.
* S-HTTP is the application of SSL over HTTP
  + Allows encryption of information passing between computers through protected and secure virtual connection

**Securing e-mail with S/MIME, PEM, and PGP**

* Secure Multipurpose Internet mail extensions builds an multipurpose internet mail extensions (MIME) encoding format by adding encryption and authentication
* Privacy enhanced mail: proposed as standard to function with public-key cryptosystems; uses 3DES symmetric key encryption
  + Uses RSA for key exchanges and digital signatures
* Pretty good privacy(PGB): uses IDEA cipher for message encoding.
  + Provides six services

**Securing web transactions with SET, SSL, and S-HTTP**

* Secure electronic transactions: developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
* Uses DES to encrypt credit card information transfers
* Provides security for both internet-based credit card transactions and credit card swipe systems in retail stores

**Securing wireless Networks with WEP and WPA**

* Wired equivalent privacy (WEP): early attempt to provide security with the 8002.11 network protocol
* Wi-Fi protected access (WPA and WPA2): created to resolve issues with WEP
* Next generation wireless protocols: robust secure networks (RSN), AES – counter mode encapsulation, AES – offset codebook encapsulation
* Bluetooth: can be exploited by anyone within approximately 30-foot range, unless suitable security controls are implemented.

**Protocols for secure communications (cont’d)**

* Securing TCP/IP with IPSec
  + Internet protocol Security (IPSec): open source protocol to secure communications across any IP-based network
  + IPSec designed to protect data integrity, user confidentially, and authenticity at IP packet level
  + IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates
  + In IPSec, IP layer security obtained by use of application header (AH) protocol or encapsulating security payload (ESP) protocol.

**Attacks on Cryptosystems**

* Attempts to gain unauthorized access to secure communications have used brute force attacks (cipher attacks)
* Attacker may alternatively conduct known-plaintext attack or selected-plaintext attack schemes

**Man-in-the-middle Attack**

* Designed to intercept transmission of public key or insert known key structure in place of requested public key
* From victim’s perspective, encrypted communication appears to be occurring normally, but in fact, attacker receives each encrypted message, decodes, encrypts and sends to originally intended recipient
* Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

**Correlation attacks**

* Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
* Differential and linear cryptanalysis have been used to mount successful attacks
* Only defense is selection of strong cryptosystems, Thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys

**Dictionary Attacks**

* Attacker encrypts every word in a dictionary using same cryptosystem used by target
* Dictionary attacks can be successful when the ciphertext consists of relatively few characters

**Timing Attacks**

* Attacker eavesdrops during victim’s session
  + Uses statistical analysis of user’s typing patterns and inter-keystroke timings to discern sensitive session information
* Can be used to gain information about encryption key and possibly cryptosystem in use
* Once encryption successfully broke, attacker may launch a replay attack

# SESSION 3: The Need for Security

**Introduction**

* Primary mission of information security is to ensure systems and contents stay the same
* If no threats existed, resources could be focused on improving systems, resulting in vast improvements in ease of use and usefulness
* Attacks on information systems are daily occurrence.

**Business Needs First**

* Information security performs four important functions for an organization:
  + Protecting the organization’s ability to function
  + Protecting the data and information the organization collects and uses
  + Safeguarding the organization’s technology’s assets in use

**Protecting the Functionality of an Organization**

* Management (general and IT) responsible for implementation
* Information security is both management issue and people issue
* Organization should address information security in terms of business impact and cost

**Enabling the Safe Operation of Applications**

* Organization needs environments that safeguard applications using IT systems
* Management must continue to oversee infrastructure once in place – not relegate to IT department

**Protecting Data that Organizations Collect and Use**

* Organization, without data, loses its record of transactions and/or ability to deliver value to customers
* Protecting data in motion and data at rest are both critical aspects of information security.
* The value of data motivates attackers to steal, sabotage, or corrupt it.

**Safeguarding technology assets in organizations**

* Organizations must have secure infrastructure services based on size and scope of enterprise
* Additional security services may be needed as organization grows
* More robust solutions may be needed to replace security programs the organization has outgrown

**Threats**

* Threat: an object, person, or other entity that represents a constant danger to an asset
* Attack: an ongoing act against an asset that could result in a loss of its value
* Exploit: a vulnerability
* Threat agent: a person or other entity that may cause a loss in an asset’s value
* Management must be informed of the different threats facing the organization
* Overall security is improving (in %)

**Compromises to Intellectual Property**

* Intellectual property (IP): “ownership of ideas and control over the tangible or virtual representation of those ideas”
* The most common IP breaches involve software piracy
* Two watchdog organizations investigate software abuse:
  + Software and information industry association
  + Business software alliance
* Enforcement of copyright law has been attempted with technical security mechanisms.

**Deliberate software attacks**

* Malicious software (malware) designed to damage, destroy, or deny service to target systems
* Includes:
  + Viruses – A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems, spreading by multiple communications vectors.
  + Worms – a type of malware that is capable of activation and replication without being attached to an existing program
  + Trojan horses – A malware program that hides its true nature and reveals its designed behaviour only when activated
  + Logic bombs – a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects
  + Back door or trap door – a malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designed to facilitate development.
  + Polymorphic threats – Threat evolves, changing its size and other external file characteristics to elude detection by antivirus software programs.
  + Virus and worm hoaxes

**Deviations in Quality of Service**

* Includes situations where products or services are not delivered as expected
* Information system depends on many interdependent support systems
* Internet service, communications, and power irregularities dramatically affect availability of information and systems

**Deviations in Quality of Service (cont’d)**

* Internet service issues
  + Internet service provider(ISP) failures can considerably undermine availability of information
  + Outsourced web hosting provider assumes responsibility for all internet services as well as hardware and web site operating system software.
* Communications and other service provider issues
  + Other utility services affect organizations: telephone, water, wastewater, trash pickup, etc.
  + Loss of these services can affect organization’s ability to function.

**Deviations in Quality of Service (cont’d)**

* Power irregularities
  + Commonplace
  + Organizations with inadequately conditioned power are susceptible
  + Controls can be applied to manage power
  + Fluctuations
    - Excess – voltage increase
    - Shortages – low voltage
    - Losses – loss of power

**Espionage or Trespass**

* Unauthorized person gains access to information an organization is trying to protect
  + The act is categorized as espionage or trespass
* Competitive intelligence – Collection and analysis of information about an organizations business competitors (legal) – means of business intelligence and competitive advantage
* Industrial espionage – collection and analysis of information about an organizations business competitors (spying) illegal.
* Shoulder surfing – covert observation of individual information or system use
* Hackers use skill, guile, or fraud to bypass controls protecting others information
* Expert hacker – uses extensive knowledge of the inner workings of computer hardware/software to gain unauthorized access to systems. Often create automated scripts.
* Unskilled hacker – uses the work of expert hackers to perform attacks. Include script kiddies and packet monkeys. Don’t fully understand the system they are hacking.

**Forces of Nature**

* Present most dangerous threats because they usually occur with little warning and are beyond the control of people w
* Can disrupt not only people’s lives but the storage, transmission, and use of information
* Organizations must implement controls to limit damage and prepare contingency plans for continued operations

**Human Error or failure**

* Acts performed without intent or malicious purpose
* Causes include:
  + Inexperience
  + Improper training
  + Incorrect assumptions
* Employees are amongst the greatest threats to an organization, employees use data and information in everyday activities to conduct the organization’s business.
* These mistakes can lead to serious threat to CIA of data.

**Information Extortion**

* The act of an attacker or trusted inside who steals information from a computer system and demands compensation for its return.

**Sabotage or Vandalism**

* Deliberate sabotage of a computer system or business
* Acts of vandalism to destroy an asset or damage the image of an organization.
* Threat of hacktivist or cyber activist operations rising
* Cyberterrorism: much more sinister form of hacking

**Technological obsolescence**

* Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems
* Proper managerial planning should prevent technology obsolescence

**Attacks**

* Acts or actions that exploits vulnerability in a controlled system
* Accomplished by threat agent that damages or steals organization’s information
* Types of attacks
  + Malicious code: includes execution of viruses, worms, Trojan horses, and active web scripts
  + Hoaxes: transmission of a virus hoax with a real virus attached
  + Back door: gaining access to a system or network using known or previously unknown/newly discovered access mechanism
  + Password crack: attempting to reverse calculate a password
  + Brute force: trying every possible combination of options of a password
  + Dictionary: selects specific accounts to attack and uses commonly used passwords to guide guesses
  + Denial-of-service(DoS): attacker sends large number of connection or information requests to a target
  + Distributed denial-of-service(DDoS): coordinated stream of requests to a target
  + Spoofing: techniques used to gain unauthorized access; intruder assumes a trusted IP address
  + Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network
  + Spam: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks
  + Mail bombing: also, a DoS; attacker routes large quantities of e-mail to target.
  + Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
  + Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity
  + Pharming: redirection of legitimate web traffic to illegitimate site for the purpose of obtaining private information

**Attacks**

* Security issues discussed here are caused by software elements of system
* Development of software and systems is often accomplished using methodology such as systems development life cycle (SDLC)
* Many organizations recognize need for security objectives in SDLC and have included procedures to create more secure software.
* This software development approach known as software assurance (SA)

**Software assurance**

* Software assurance is a methodological approach to the development of software that seeks to build security into the development life cycle rather than address it at later stages.

**Software Design Principles**

* Commonplace security principles:
  + Keep design simple and small
  + Access decisions by permission not exclusion
  + Every access to every object checked for authority
  + Design depends on possession of keys/passwords
  + Protection mechanisms require two keys to unlock
  + Programs/users utilize only necessary privileges
  + Minimize mechanisms common to multiple users
  + Human interface must be easy to use so users routinely/automatically use protection mechanisms

# SESSION 4: Legal, Ethical, and professional issues in Information Security

**Laws and Ethics in Information Security**

* Laws: rules that mandate or prohibit certain societal behaviour
* Ethics: define socially acceptable behaviour
  + Some ethics are recognized as universal among cultures
* Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these
* Laws carry sanctions of governing authority

**Organizational Liability and the need for Counsel**

* Due care: Insuring that employees know what constitutes acceptable behaviour and know the consequences of illegal or unethical actions
* Due diligence: making a valid effort to protect others; continually maintaining level of effort.
* Jurisdiction: a court’s right to hear a case if a wrong is committed in its territory or involves its citizenry
* Liability: the legal obligation of an entity that extends beyond criminal or contract law
* Long-arm jurisdiction: right of any court to impose its authority over an individual or organization if it can establish jurisdiction
* Restitution: Compensate for wrongs committed by an organization or its employees.

**Policy versus law**

* Policies: Managerial directives that specify acceptable and unacceptable employee behaviour in the workplace.
* Policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate and fairly applied to everyone in the workplace.
* Difference between a policy and a law is that policy outlines what a government ministry hopes to achieve and the methods and principles it will use to achieve them. Laws set out standards, procedures and principles that must be followed.
* Criteria for policy enforcement:
  + Dissemination (distribution): The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee.
  + Review(reading): The organization must be able to demonstrate that it disseminated the document in an intelligible form.
  + Comprehension(understanding): The organization must be able to demonstrate that the employee understands the requirements and content of the policy.
  + Uniform environment: The organization must be able to demonstrate that the policy has been uniformly

**Types of law**

* Civil: governs nation or state; manages relationships/conflicts between organizational entities and people
* Criminal: addresses violations harmful to society actively enforced by the state
* Private: regulates relationships between individuals and organizations
* Public: regulates structure/administration of government agencies and relationships with citizens, employees, and other governments.

**General computer crime laws**

* Computer Fraud and Abuse Act of 1986 (CFA Act):
  + Cornerstone of many computer-related federal laws and enforcement efforts
  + National information infrastructure Protection act of 1996:
    - Modified several sections on the previous act and increased the penalties for selected crimes

**Privacy**

* Is a “state of being free from unsanctioned intrusion”
* Ability to aggregate data from multiple sources allows creation of information databases previously impossible.
* The number of statuses addressing an individual’s right to privacy has grown.
* Identity theft:
  + Attempts to instigate penalties for identity theft by recognizing people who lose their identity as the true victims, not just the commercial and financial credit entitles that suffered losses.
* NZ Privacy act:
  + Personal information is only to be collected for a lawful purpose connected with a function or activity of the agency.
  + Information should be collected directly from the individual concerned
  + The individual concerned should be aware that information is being collected and should know:
    - The purpose for which the information is being collected
    - Who are the intended recipients of the information?
    - The consequences for the individual if the information is not provided
    - The rights of access to and correction of personal information provided
  + Personal information shall not be collected by unlawful or unfair or intrusive means
  + Information is protected by security safeguards against loss, unauthorised access, use, disclosure or modification.
  + The individual concerned shall be entitled to obtain confirmation that information is held and access to information held.
  + The holder of personal information must check its accuracy before use.
  + Information may only be used for the purpose for which it was originally intended
  + The holder of personal information may not disclose that information to any other person or agency
  + The holder of personal information may not assign a unique unless it is necessary to carry out its function, nor may that identifier be that already used by another holder.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

* Protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.
* Consumer control of medical information
* Boundaries on the use of medical information
* Accountability for the privacy of private information
* Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
* Security of health information.

**Copyright Law**

* Intellectual property recognized as protected asset in many countries, like: NZ, AUS, USA; copyright law extends to electronic formats
* With proper acknowledge, permissible to include portions of others work as reference

**Financial Reporting**

* Sarbanes-Oxley Act of 2002:
  + Seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.

**State and Local Regulations**

* Information security professionals must understand state laws and regulations and ensure that their organizations security policies and procedures are in compliance.

**Informational laws and legal bodies**

* When organizations do business on the internet, they do business globally
* Professionals must be sensitive to laws and ethical values of many different cultures, societies, and countries.
* Because of political complexities of relationships among nations and differences in culture, there are few international laws relating to privacy and information security.
* These international laws are important but are limited in their enforceability.

**Ethics and information security**

* Many Professional groups have explicit rules governing ethical behaviour in the workplace
* IT and IT security do not have binding codes of ethics
* Professional associations and certification agencies work to establish codes of ethics

# SESSION 5: Planning for Security

* Information security program begins with policies, standards, and practices, which are the foundation for information security architecture and blueprint
* Coordinated planning required to create and maintain these elements
* Strategic planning for management of allocation of resources
* Contingency planning for preparation of uncertain business environment.

**Information security planning and governance**

* Planning levels help translate organization’s strategic plans into tactic objectives
* Planning and the CISO
* Information Security Governance
  + Governance:
    - Set of responsibilities and practices exercised by the board and executive management.
    - Goal to provide strategic direction, establishment of objectives, and measurement of progress toward objectives.
    - Also verifies / validates that risk management practices are appropriate and assets used properly.
* Information Security Governance outcomes
* Five goals:
  + Strategic alignment
  + Risk management
  + Performance measures
  + Value delivery
  + Resource management

**Roles and responsibilities**

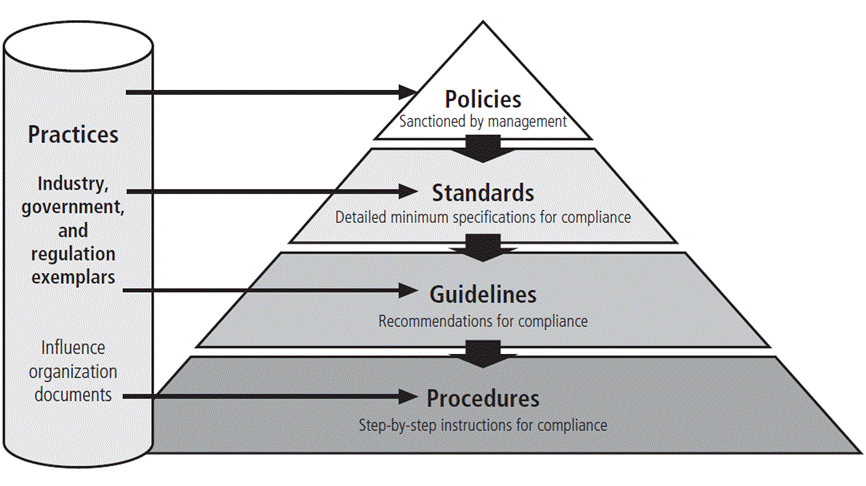
* A set of responsibilities relate to a function role
* This table collects what the functions are in terms of responsibilities of workers.
* Right hand side has 7 different types of jobs
* Left hand side are what sort of jobs are assigned to the rules.

**Information security policy, standards and practices**

* Management from communities of interest must make policies the basic for all information security planning, design, and deployment.
* Policies direct how issues should be addresses and technologies used.
* Policies should never contradict law, must be able to stand up in court, and must be properly administered.
* Security policies are the least expensive controls to execute but most difficult to implement properly.

**Policy as the Foundation for Planning**

* Policy functions as organizational law that dictates acceptable and unacceptable behaviour.
* Standards: more detailed statements of what must be done to comply with policy
* Practices, procedures and guidelines effectively explain how to comply with policy.
* For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of the organisation, and uniformly enforced.



* Policies are for the people in a high position (set by them)
* Standards- internal set up by the company or national or international, these are the suggested way general activity is managed.
* If you are a regular company you don't have to follow the standard but there is a problem.
* Government department must follow those standards
* Guidelines which way an operation can be carried

**Enterprise information security policy**

* Sets strategic direction, scope, and tone for all security efforts within the organization.
* Executive-level document, usually drafted by or with Chief Information Officer (CIO) of the organization
* Typically addresses compliance in two areas:
  + Ensure meeting of requirements to establish program and assigning responsibilities there in to various organizational components.
  + Use of specified penalties and disciplinary action
* EISP Elements should include:
  + Overview of corporate security philosophy
  + Information on the structure of the organization and people in information security roles
  + Articulated responsibilities for security shared by all members of the organization
  + Articulated responsibilities for security unique to each role in the organization

**Issue-Specific Security Policy**

* The ISSP:
  + Addresses specific areas of technology
  + Requires frequent updates
  + Contains statement on the organization’s positions on specific issue
* Three common approaches when creating and managing ISSPs:
  + Create several independent ISSP documents
  + Create a single comprehensive ISSP document
  + Create a modular ISSP document.
* Components of the policy:
  + Statement of policy
  + Authorized access and usage of equipment

**Systems-Specific Policy**

* SysSPs often function as standards or procedures used when configuring or maintaining systems.
* Systems-specific policies fall into two groups:
  + Managerial guidance
  + Technical specifications
* Access control lists can restrict access for a particular user, computer, time, duration – even a particular file
* Configuration rule policies govern how security system reacts to received data
* Combination SysSPs combine managerial guidance and technical specifications

**Policy Management**

* Polices must be managed as they constantly change
* To remain viable, security policies must have:
  + A responsible manager
  + A schedule of reviews
  + A method for making recommendations for reviews
  + A policy issuance and revision date
  + Automated policy management
* Someone needs to be responsible for managing that policy

**The Information Security Blueprint**

* Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
* Detailed version of security framework
* Specifies tasks and order in which they are to be accomplished
* Should also serve as a scalable, upgradable, and comprehensive plan for the current and future information security needs.

**The ISO 27000 Series**

* One of the most widely referenced security models
* Standard framework for information security that states organizational security policy is needed to provide management direction and support
* Purpose is to give recommendations for information security management
* Provides a starting point for developing organizational security

**Design of Security Architecture**

* Spheres of security: foundation of the security framework
* Levels of controls
  + Management controls set the direction and scope of the security processes and provide detailed instructions for its conduct.
  + Operational controls address personnel and physical security, and the protection of production inputs/outputs
  + Technical controls are the tactical and technical implementations related to designing and integrating security in the organization.
* Defence in depth
  + Implementation of security in layers.
  + Requires that organisation establish multiple layers of security controls and safeguards.
* Security perimeter
  + Border of security protecting internal systems from outside threats
  + Does not protect against internal attacks from employee threats or onsite physical threats.

**Security Education, Education, Training and Awareness Program**

* Once general security policy exists, implement security education, training, and awareness (SETA) program.
* SETA is a control measure designed to reduce accidental security breaches.
* The SETA program consists of security education, security training, and security awareness.
* Enhances security by improving awareness, developing skills, and knowledge, and building in-depth knowledge.

**Security Education**

* Everyone in an organization needs to be trained and aware of information security; not every member needs a formal degree of certificate in information security.
* When formal education is deemed appropriate, an employee can investigate courses in continuing education from local institutions of higher learning.
* A number of universities have formal coursework in information security.

**Security Training**

* Provides members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
* Management of information security can develop customized in-house training or outsource the training program.
* Alternatives to formal training or outsource the training program
* Alternatives to formal training include conferences and programs offered through professional organizations.

**Security Awareness**

* One of the least frequently implemented but most beneficial programs is the security awareness program.
* Designed to keep information security at the forefront of users’ minds
* Need not be complicated or expensive
* If the program is not actively implemented, employees may begin to neglect security matters, and risk of employee accidents and failures are likely to increase.

**Continuity Strategies**

* Incident response plans (IRPs); disaster recovery plans (DRPs); business continuity plans(BCPs)
* Primary functions of above plans:
  + IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP
  + DRP typically focuses on restoring systems after disasters occur; as such, it is closely associated with BCP.
  + BCP occurs concurrently with DRP when damage is major or ongoing, requiring more than simple restoration of information and information resources.

**Continuity Strategies**

* Before planning can actually begin, a team has to start the process.
* Champion: high-level manager to support, promote, and endorse findings of the project.
* Project manager: leads project and ensures sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed.
* Team members: should be managers, or their representatives, from various communities of interest: business, IT, and information security.

**Contingency Planning (CP) process**

* Includes the following steps:
  + Develop CP policy statement
  + Conduct business impact analysis
  + Identify preventive controls
  + Create contingency strategies
  + Develop contingency plan
  + Ensure plan testing, training, and exercises
  + Ensure plan maintenance

**CP Policy**

* Should contain the following sections:
  + Introductory statement of philosophical perspective
  + Statement of scope/purpose
  + Call for periodic risk assessment/BIA
  + Specification of CP’s major components
  + Call for/guidance in the selection of recovery options
  + Requirement to test the various plans regularly
  + Identification of key regulations and standards
  + Identification of key people responsible for CP operations
  + Challenge to the organization members for support
  + Administrative information

**Business Impact Analysis (BIA)**

* Investigation and assessment of various adverse events that can affect organization
* Assumes security controls have been bypassed, have failed, or have proven ineffective, and attack has succeeded
* Organization should consider scope, plan, balance, knowledge of objectives, and follow-ups
* Three stages:
  + Determine mission/ business processes and recovery criticality
  + Identify recovery priorities for system resources
  + Identify resource requirements

**Incident Response Planning**

* Incident response planning includes identification of, classification of, and response to an incident.
* Attacks classified as incidents if they:
  + Are directed against information assets
  + Have a realistic chance of success
  + Could threaten confidentiality, integrity, or availability of information resources.
  + Could threaten confidentiality, integrity or availability of information resources.
  + Incident response (IR) is more reactive than proactive, except for planning that must occur to prepare IR teams to be ready to react to an incident.
* Incident response policy identifies the following key components:
  + Statement of management commitment
  + Purpose/objectives of policy
  + Scope of policy
  + Definition of InfoSec incidents and related terms
  + Organizational structure
  + Prioritization or severity ratings of incidents
  + Performance measures
  + Reporting and contact forms
* Incident Planning
  + Predefined responses enable the organization to react quickly and effectively to the detected incident if:
    - The organization has an IR team
    - The organization can detect the incident
  + IR team consists of individuals needed to handle systems as incident takes place.
* Incident response plan
  + Format and content
  + Storage
  + Testing
* Incident detection
  + Most common occurrence is complaint about technology support, often delivered to help desk.
  + Careful training is needed to quickly identify and classify an incident
  + Once incident is properly identified, the organization can respond.
  + Incident indicators vary.
* Incident reaction
  + Consists of actions that guide the organization to stop incident, mitigate its impact, and provide information for recovery
  + Actions that must occur quickly:
    - Notification of key personnel
    - Documentation of the incident
* Incident containment strategies
  + Containment of incident’s scope or impact as priority; must then determine which information systems are affected.
  + Organization can stop incident and attempt to recover control through a number of strategies.
* Incident recovery
  + Once incident has been contained and control of systems regained, the next stage is recovery.
  + The first task is to identify human resources needed and launch them into action.
  + Full extend of the damage must be assessed.
  + Organization repairs vulnerabilities, addresses any shortcomings in safeguards, and restores data and services of the systems.
* Damage assessment
  + Several sources of information on damage can be used, including system logs, intrusion detection logs, configuration logs, and documents, documentation from incident response, and results of detailed assessment of systems and data storage.
  + Computer evidence must be carefully collected, documented, and maintained to be usable in formal or informal proceedings.
  + Individuals who assess damage need special training.
* Automated response
  + New systems can respond to incident threat autonomously.
  + Downsides of current automated response systems may outweigh benefits.
    - Legal abilities of a counterattack
    - Ethical issues

**Disaster Recovery Planning**

* Disaster recovery planning (DRP) is preparation for and recovery from a disaster.
* The contingency planning team must decide which actions constitute disasters and which constitute incidents.
* When situations are classified as disasters, plans change as to how to respond; act to secure most valuable assets to preserve value for the longer term.
* DRP strives to re-establish operations at the primary site.

**Business Continuity Planning**

* Prepares the organization to re-establish or relocate critical business operations during a disaster that affects operations at the primary site.
* If disaster has rendered the current location unusable, there must be a plan to allow business to continue functioning
* Development of BCP is somewhat simpler than IRP or DRP.
  + Consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy.
* Continuity strategies
  + There are a number of strategies for planning for business continuity
  + Determining factor in selecting between options is usually cost.
  + In general, there are three exclusive options:
    - Hot sites
    - Warm sites
    - Cold sites
  + Three shared functions: time-share, service bureaus, and mutual agreements.
* Off-site disaster data storage
  + To get sites up and running quickly, an organization must have the ability to move data into new site’s systems.
  + Options for getting operations up and running include:
    - Electronic vaulting
    - Remote journaling
    - Database shadowing

**Crisis management**

* Actions taken in response to emergency to minimize injury/loss of life, preserve organization’s image/market share, and complement disaster recovery/business continuity processes
* What may truly distinguish an incident from a disaster are the actions of the response teams.
* Disaster recovery personnel must know their roles without any supporting documentation
  + Preparation
  + Training
  + Rehearsal
* Crisis management team is responsible for managing the event from the enterprise perspective and covers:
  + Supporting personnel and families during crisis
  + Determining impact on normal business operations and, if necessary, making disaster declaration
  + Keeping the public informed
  + Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other parties.

# SESSION 6: Security Technology: Firewalls and VPNs

**Access control**

* Access control: Method by which systems determine whether and how to admit a user into a trusted area of the organization
* Mandatory access control (MACs): use data classification schemes
* Discretionary access controls (DACs): allow users to control and possibly provide access to information/ resources at their disposal.
  + Controlled by user
* Nondiscretionary controls: strictly enforced version of MACs that are managed by a central authority.
  + Controlled by organization

**Identification**

* Identification: mechanism whereby unverified entities seeking access to a resource (supplicants) provide a label by which they are known to the system.
* Identifiers can be composite identifiers, concatenating elements – department codes, random numbers, or special characters – to make them unique.
* Some organizations generate random numbers
* Gaining access to a system involves identification and authentication. Identification tells the system who you are.

**Authentication**

* Authentication: the process of validating a supplicant’s purported identity
* Authentication factors
  + Something a supplicant knows
    - Password: a private word or a combination of characters that only the user should know.
    - Passphrase: a series of characters, typically longer than a password, from which a virtual password is derived.
* Authentication: involves password, can also be that you carry something which provides the authentication or it may be physical characteristic (retina, finger-print, etc)
* Authentication factors
  + Something a supplicant has
    - Dumb card: ID or ATM card with magnetic stripe
    - Smart card: contains a computer chip that can verify and validate information
    - Synchronous tokens
    - Asynchronous tokens
  + Something a supplicant is
    - Relies upon individual characteristics
    - Strong authentication
  + Synchronous – usually a timer which works simultaneously

**Authorization**

* Authorization: The matching of an authenticated entity to a list of information assets and corresponding access levels
* Authorization can be handled in one of three ways:
  + Authorization for each authenticated user
  + Authorization for members of a group
  + Authorization across multiple systems
* Authorization tickets

**Accountability**

* Accountability (auditability): ensures that all actions on a system = authorized or unauthorized – can be attributed to an authenticated identity.
* Most often accomplished by means of system logs and database journals, and the auditing of these records
* System logs record specific information
* Logs have many users

**Biometrics**

* Approach based on the use of measurable human characteristics/traits to authenticate identity
* Only fingerprints, retina of eye, and iris of eye are considered truly unique.
* Evaluated on false reject rate, false accept rate, and crossover error rate.
* Highly reliable/effective biometric systems are often considered intrusive by users.
* Great if you However, for sensitive application biometrics is a dangerous thing to do, if someone finds out your old code you are comprised for life (e.g. finger tips, retina, etc.) Access control Architecture Models
* Illustrate access control implementations and can help organizations quickly make improvements through adaptation
* Trusted computing base(TCB)

# Part of TCSEC Rainbow Series

# Used to enforce security policy (rules of system configuration)

# Biggest challenges include covert channels

# Storage channels

# Timing channels

**Access control**

* ITSEC: an international set of criteria for evaluating computer systems
  + Compares targets of Evaluation (ToE) to detailed security function specifications
* The Common criteria
  + Considered successor to both TCSEC and ITSEC
* Bell-LaPadula Confidentiality Model
  + Model of an automated system able to manipulate its state or status over time
* Biba integrity Model
  + Based on “no write up, no read down” principle
* Not allowed to write into security log
  + Stop spreading confidential information
* Biba Integrity Model – pretty much the same as bell model in terms of integrity

**Architecture Models**

* Clark-Wilson Integrity Model
  + No changes by unauthorized subjects
  + No unauthorized changes by authorized subjects
  + Maintenance of internal and external consistency
* Brewer-Nash Model (Chinese wall)
  + Designed to prevent conflict of interest between two parties

**Firewalls**

* Prevent specific types of information from moving between an untrusted network (the internet) and a trusted network (organization’s internal network)
* May be:
  + Separate computer system
  + Software service running on existing router or server
  + Separate network containing supporting devices
* Filter which may have different characteristic depending on traffic
* Firewalls filters only two parameters (address of messages where it comes from what sort of service it is/provides)

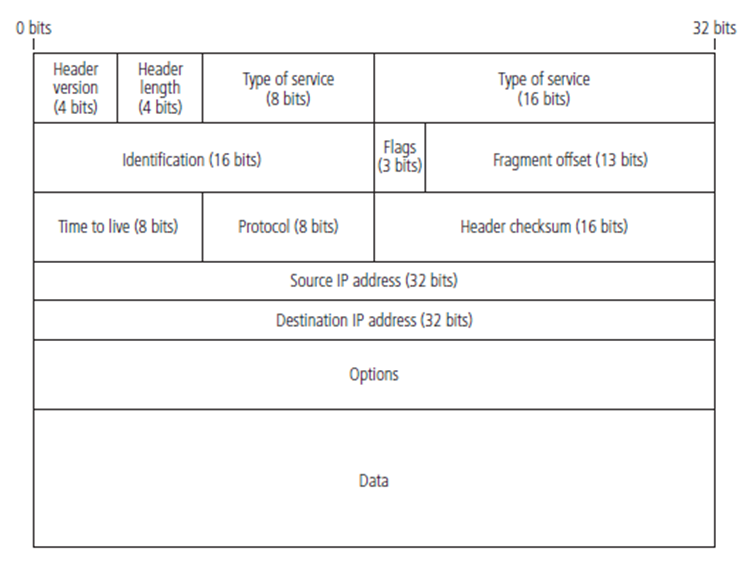
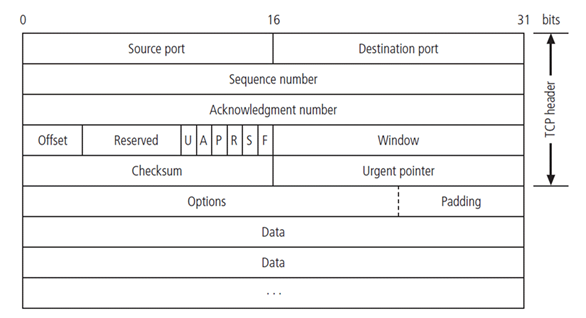
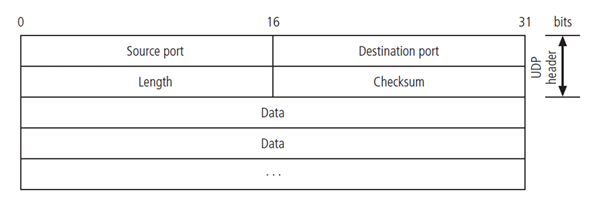
**Firewalls processing modes**

* Five processing modes by which firewalls can be categorized:
  + Packet filtering
  + Application gateways
  + Circuit gateways
  + MAC layer firewalls
  + Hybrids

**Packet-Filtering firewalls**

* Packet-filtering firewalls examine the header information of data packets.
* Most often based on the combination of:
  + IP source and destination address
  + Direction (inbound or outbound)
  + Transmission control protocol (TCP) or User Datagram Protocol(UDP) source and destination port requests
* Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

Packet-filtering Firewalls

* Packet-filtering firewalls examine the header information of data packets.
* Most often based on the combination of:
  + IP source and destination address
  + Direction (inbound or outbound)
  + Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests
* Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.
* We are looking for source and destination IP addresses, interest of the firewall.
* Looking for source and destination port! Port is the name that tells us what type of service is inside the given packet.
* Also look at sequence number
* Packet-filtering router – should we allow given packets to travel or reject it.
  + Firewall rules will have source address (ip address), destination address, service (protocol) and your action to deny or allow it.
  + Role of firewall is to allow data to flow

**Packet-Filtering Firewalls (cont’d)**

* Three subsets of packet-filtering firewalls:
  + Static filtering: requires that filtering rules be developed and installed within the firewall
  + Dynamic filtering: allows firewall to react to emergent event and update or create rules to deal with event.
  + Stateful inspection: firewalls that keep track of each network connection between internal and external systems using a state table.

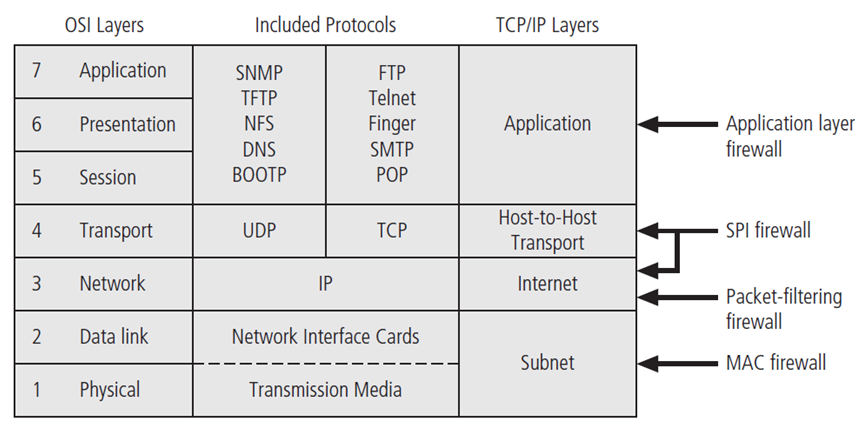
**Application Layer Firewall**

* Frequently installed on a dedicated computer; also known as a proxy server
* Since proxy server is often placed in unsecured area of the network, it is exposed to higher levels of risk from less trusted networks.

Additional filtering routers can be implemented behind the proxy server, further protecting internal systems.

**Firewall Processing modes (cont’d)**

* MAC layer firewalls
  + Designed to operate at media access control sublayer of network’s data link layer
  + Make filtering decisions based on specific host computer’s identity
  + MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked.
* Hybrid firewalls
  + Combine elements of other types of firewalls, that is elements of packet filtering and proxy services, or of packet filtering and circuit gateways.



**Firewall Architectures**

* Firewall devices can be configured in several network connection architectures.
* Best configuration depends on three factors:
  + Objectives of the network
  + Organization’s ability to develop and implement architectures
  + Budget available for function
* Four common architectural implementations of firewalls: packet-filtering routers, dual-homed firewalls (bastion hosts), screened host firewalls, screened subnet firewalls
* Settings of firewalls are very important and must align with the business.

**Firewall Architectures (cont’d)**

* Packet-filtering routers
  + Most organizations with internet connection have an outer at the boundary between internal networks and external service provider.
  + They can be configured to reject packets that the org doesn’t allow in the network.
* Bastion hosts
  + Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
  + Contains two network interface cards (NICs): one connected to external network, one connected to internal network
  + Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers

**Firewall Architectures**

* Screened subnet performs two functions
  + Protects DMZ systems and outside threats
  + Protects internal networks by limiting how external connections can gain access to internal systems

**Selecting the right firewall**

* When selecting the firewall, we consider several factors:
  + Firewall technology, balance between protection and cost for the needs of the company
  + Features in base price
  + Easy to set up and configure
    - Accessible to staff and who can configure the firewall
  + Can firewall adapt to companies growing network
* Second most important issue is cost

**Configuring and Managing firewalls**

* The organization must provide for the initial configuration and ongoing management of firewall(s)
* Each firewall device must have its own set of configuration rules regulating its actions
* Firewall policy configuration is usually complex and difficult
* Configuring firewall policies is both an art and a science
* When security rules conflict with the performance of business, security often loses.
* Best practices for firewalls:
  + All traffic from the trusted network is allowed out
  + Firewall device is never directly accessed from public network
  + SMTP data are allowed to pass through firewall
  + ICMP data are denied
  + Telnet access to internal servers should be blocked
  + When web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks
  + All data not verifiably authentic should be denied.

**Content Filters**

* Software filter – not a firewall – that allows administrators to restrict content access from within a network
* Essentially a set of scripts or programs restricting user access to certain networking protocols/internet locations
* Primary purpose to restrict internal access to external material
* Most common content filters restrict users from accessing non-business website or deny incoming spam

**Remote access**

* Dial-up connection points represent substantial exposure to attack
* War dialer can be used to locate connection points
* Radius, Diameter and TACACS
  + Systems that authenticate user credentials for those trying to access an organizations network via dial-up
  + Remote Authentication Dial-In User Service (RADIUS): centralizes responsibility for user authentication in a central RADIUS server.
* Kerberos
  + Provides secure third-party authentication
  + Uses symmetric key encryption to validate individual user to various network resources
  + Quick and efficient

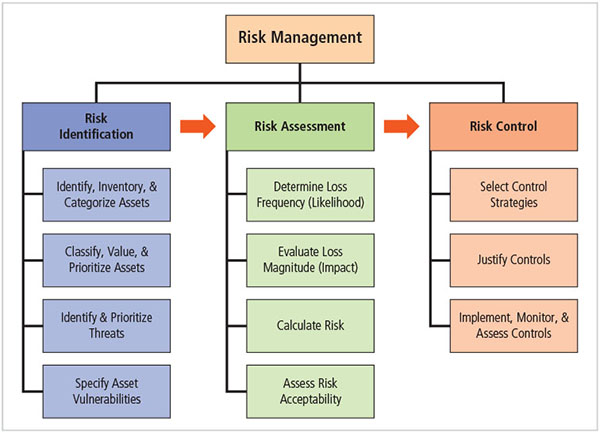
**Virtual Private Networks(VPNs)**

* Private and secure network connection between systems; uses data communication capability of unsecured and public network
* Securely extends organization’s internal network connections to remote locations
* Three VPN techs defined:
  + Trusted VPN
  + Secure VPN
  + Hybrid VPN
* VPN must accomplish:
  + Encapsulation of incoming and outgoing data
  + Encryption of incoming and outgoing data
  + Authentication of remote computer and perhaps remote user as well
    - It allows the user to turn internet into a private network.
* Transport mode
  + Data within IP packets is encrypted, but header information is not.

# SESSION 7: Risk Management

**Risk Management**

* Risk management: the process of identifying, assessing, and reducing risks facing an organization
* Risk identification: the enumeration and documentation of risks to an organizations information asset
* Risk control: The application of controls that reduce the risk to an organization’s assets to an acceptable level



* Risk identification
  + What can go wrong
* Risk assessment
  + What can happen
* Risk control
  + The damage

The more you invest the better you are protected.

**Risk Appetite and Residual Risk**

* Risk appetite it defines the quantity and nature of risk that organizations are willing to accept as trade-offs between perfect security and unlimited accessibility
  + Reasoned approach is one that balances the expense of controlling vulnerabilities against possible losses if the vulnerabilities are exploited.
* Residual risk: risk that has not been completely removed, shifted, or planned for
  + The goal of information security is to bring residual risk into line with risk appetite.

**Identifying, inventorying, and categorizing assets**

* Iterative process: begins with the identification and inventory of assets, including all elements of an organization’s systems (people, procedures, data and information, software, hardware, networking)
* Assets are then categorized.

**People, Procedures, and Data Asset Identification**

* Human resources, documentation, and data information assets are more difficult to identify
* Important asset attributes:
  + People
  + Procedures: description, relation to software/hardware
  + Data

**Hardware, software and network asset identification**

* What information attributes to track depends on:
  + Needs of organization/risk management efforts
  + Preferences/needs of the security and information technology communities.
* Attributes to be considered are: IP address, MAC address, element type, serial number etc.

**Asset Categorization**

* People comprise employees etc.
* Data components account for the management of information in transmission, processing, and storage
* Software components are applications, operating systems, or security components

**Data classification and Management**

* Variety of classification schemes are used by corporate and military organizations.
* Information owners are responsible for classifying their information assets.
* Information classifications must be reviewed periodically.
* Security clearances

**Information asset valuation**

* Questions help develop criteria for asset valuation
* Which information asset:
  + Is most critical to the organizations success
  + Generates the most revenue
  + Would be the most expensive

**Risk Assessment**

* Risk assessment evaluates the relative risk for each vulnerability
* It assigns a risk rating or score to each information asset
* Planning and organizing risk assessment
  + The goal at this point is to create a method for evaluating the relative risk of each listed vulnerability

**Determining the loss frequency**

* Describes an assessment of the likelihood of an attack combined with expected probability of success
* Use external references for values that have been reviewed/adjusted for your circumstances
* Assign numeric value to likelihood typically annual value.

**Factors of risk (will be in test)**

* Risk is:
  + The probability of a successful attack on the organization
  + (loss frequency = likelihood \* attack success probability)
    - Multiplied by the expected loss from a successful attack
    - (loss magnitude = asset value \* probable loss) plus the uncertainty of estimates of all stated values

**Defence**

* Attempts to prevent exploitation of the vulnerability
* Countering threats, removing asset vulnerabilities
* Three methods of risk avoidance:
  + Application of policy
  + Education and training
  + Applying technology

**Transference**

* This strategy attempts to shift risk to other assets, processes, or organizations
* If lacking the org should hire individuals/firms that provide security management and admin expertise
* Org can transfer to another org who’s used to dealing with these risks

**Acceptance and termination**

* Acceptance
  + Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
  + Valid only when the function, service, information, or asset does not justify the cost of protection.
* Termination
  + Directs the organization to avoid business activities that introduce uncontrollable risks

**The Cost-Benefit Analysis (CBA) formula (will be in test)**

* CBA determines if an alternative being evaluated is worth the cost incurred to control vulnerability
  + The CBA is most easily calculated using the ALE from earlier assessments, before implementation of the proposed control:
    - CBA = ALE(prior) – ALE(post) – ACS
  + ALE(prior) is the annualized loss expectancy of risk before implementation of control
  + ALE(post) is the estimated ALE based on control being in place for a period of time
  + ACS is the annualized cost of the safeguard

**Benchmarking and best practices**

* An alternative approach to risk management
* Benchmarking: process of seeking out and studying practices in other organizations that one’s own organization desires to duplicate
* One of two measures typically used to compare practices:
  + Metrics-based measures based on numerical standards
* Baselining
  + Comparing what your company is doing with another company.

**Other feasibility studies**

* Organizational: Assesses how well the proposed IS alternatives will contribute to an organization’s efficiency, effectiveness, and overall operation
* Operational: Assesses user and management acceptance and support, and the overall requirements of the organization’s stakeholders
* Technical: Assesses if organization has or can acquire the technology necessary to implement and support proposed control
* Political: Defines what can/cannot occur based on the consensus and relationships among communities of interest

# SESSION 8: Intrusion detection and prevention systems, and other security tools

Intrusion Detection and Prevention Systems (1 of 2)

* An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an organization’s information systems.
* Intrusion prevention consists of procedures and systems that identify system intrusions
* Intrusion reaction encompasses actions an organization undertakes when intrusion event is detected.

Intrusion Detection and Prevention Systems (2 of 2)

* Intrusion correction activities complete restoration of operations to a normal state and seek to identify source and method of intrusion.
* Intrusion detection systems detect a violation of its configuration and activate alarm.
* Many IDPs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers
* Systems can also be configured to notify an external security services organization of a “break-in”

IDPS Terminology (1 of 2)

* Alarm clustering and compaction – Any bigger installation is almost on a permanent status of attack. Attacks may be very similar, we may try to cluster those attacks in specific groups.
* Alarm filtering – if we cluster then we will standardize the information about what had happened, to ignore confusion about the viruses and to be able to classify it.
* Alert/alarm – “easy to understand”
* Confidence value – describe what trust we have in the intrusion detection system
* Evasion – If we can somehow eliminate the possible bad influence of the attack
* False attack stimulus – are a way of testing the system of some sort of attack to see how the system reacts to this abuse
* False negative – important factor, we are being attacked successfully but we are getting no information about it
* False positive – This is simply the opposite of the above
* Noise – we may be subject of permanent attack, they may be weak. We know about the attack, but we can sustain the attack. We can filter the those attacks as low-level attacks which are called noise.

IDPS Terminology (2 of 2)

* Site policy – which way we deploy our intrusion detection system, set up settings of these systems
* Site policy awareness – People need to know what sort of measure we have implemented
* True attack stimulus – Testing our system against given type of attack (pen testing, penetration testing)
* Tuning – set up all the parameters of intrusion detection carefully

Why use an IDPS

* Intrusion detection:
  + Primary purpose to identify and report intrusion
  + Contain an attack and prevent the loss or damager
  + Detect and deal with preambles to attacks
* Data collection allows the organization to examine what happened after an intrusion and why
* Servers as a deterrent by increasing the fear of detection
* Can help management with quality assurance and continuous improvement.

Types of IDPSs (1 of 12)

* IDPSs operate as network-based or host-based systems.
* Network-based. IDPS is focused on protecting network information assets
  + Wireless IDPS focuses on wireless networks
  + Network behavior analysis IDPS examines traffic flow on a network to recognize abnormal patterns.

The cyberattack and kill chain (2 of 12)

An illustration shows various steps for Intrusion Kill chain. Seven titles in column wise and their corresponding text below them. The first topic is Reconnaissance under which the text reads as, “Research, identification, and selection of targets, often represented as crawling Internet Web sites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.” The second title is Weaponization under which the text reads as, “Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF of Microsoft Office documents serve as the weaponized deliverable.” The third title is delivery under which the text reads as, “Transmission of the weapon to the targeted environment using vectors like email attachments, Web sites, and USB removable media.” The fourth topic is Exploitation and the text below it reads as, “After the weapon is delivered to victim host, exploitation triggers intruders’ code. Most often, exploitation targets an application or operating system vulnerability.” The fifth topic is Installation and the text below it reads as, “Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.” The sixth topic is Command and control (C2) under which the text reads as, “Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel.” The seventh topic is Actions on objectives below which the text reads as, “Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration, which involves collecting, encrypting, and extracting information from the victim environment.” There are six more steps mentioned below these text horizontally. They are, “Detect, Deny, Disrupt, Degrade, Deceive and Destroy.” Below it are the two steps that reads as, “Leverage, discover, analyze and Atomic, computed, and behavior indicators.” The last step is represented in a grey block and the text reads as, “Campaign Analysis–Tools, Techniques, and procedures.”


Intrusion detection and prevention systems (3 of 12)

An illustration shows an untrusted network pointing to a router labeled as, “External router.” The router points to lens inside which an arrow with named as data and header is shown. The handle of lens is named as, “Packet flow.” A text points with an arrow points to the lens and it reads as, “Network IDPS: Examines packets on network and alerts administrators of unusual patterns.” The lens is then pointed to a CPU which divides into two computers and a CPU. A lens is shown near the main CPU in the lowers side. It is then classified into two computers on the upper side. A text points to a main CPU and it reads as, “Host IDPS: Examines the data in files stored on host and alerts systems administrators of changes.”


Types of IDPSs (4 of 12)

* Network-based IDPS (NIDPS)
  + Resides on a computer or an appliance connected to a segment of an organization’s network; looks for indications of attacks
  + When examining packets, an NIDPS looks for attack patterns within network traffic
  + Installed at specific place in the network where it can monitor traffic going into and out of a network segment.

Types of IDPSs (5 of 12)

* Network-based IDPS (NIDPS) (cont’d)
  + To determine whether attack has occurred or is under way, compare measured activity to known signatures in knowledge base.
  + Done by using special implementation of TCP/IP stack:
    - In the process of protocol stack verification, NIDPSs look for invalid data packets.
    - In the application protocol verification, higher-order protocols are examined for unexpected packet behaviour or improper use.
  + Should not slow down the system, it may be complicated as variety of messages into an organization can be enormous.
  + Setting up detection system can be difficult

Types of IDPSs (6 of 12)

* Advantages of NIDPs
  + Good network design and placement of NIDPS can enable an organization to monitor a large network with few devices
  + NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal operations
  + NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers

Types of IDPSs (7 of 12)

* Disadvantages of NIDPSs
  + Can become overwhelmed by network volume and fail to recognize attacks
  + Require access to all traffic to be monitored
  + Cannot analyse encrypted packets
  + Cannot reliably ascertain if an attack was successful or not
  + Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets.

Types of IDPSs (8 of 12)

* Wireless NIDPS
  + Monitors and analyses wireless network traffic
  + Issues associated with it include physical security, sensor range, access point and wireless switch locations, wired network connections, cost, AP, and wireless switch locations
* Network behaviour analysis systems
  + Identify problems related to the flow of traffic

Types of IDPSs (9 of 12)

* Types of events commonly detected include denial-of-service (DoS) attacks, scanning, worms, unexpected application services, and policy violations
* Offer intrusion prevention capabilities that are passive, inline, and both passive and inline.

Types of IDPSs (10 of 12)

* Host-based IDPS (HIDPS)
  + Resides on a computer or server (host) and monitors activity only on that system
  + Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files.
  + Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks
  + Most HIDPSs work on the principle of configuration or change management

Types of IDPSs (11 of 12)

* Advantages of HIDPSs
  + Can detect local events on host systems and detect attacks that may elude a network-based IDPS
  + Functions on host system, where encrypted traffic would have been decrypted and is available for processing
  + Not affected by use of switched network protocols
  + Can detect inconsistencies in how applications and system programs were used by examining records stored in audit logs

Types of IDPSs (12 of 12)

* Disadvantages of HIDPSs
  + Pose more management issues
  + Vulnerable both to direct attacks and attacks against the host operating system
  + Does not detect multihost scanning, nor scanning of non-host network devices
  + Susceptible to some DoS attacks
  + Can use large amounts of disk space
  + Can inflict a performance overhead on its host systems

IDPSs Detection Methods (1 of 4)

* Signature-based detection (or knowledge based detection or misuse detection)
  + Examines network traffic in search of patterns that match known signatures
  + Widely used because many attacks have clear and distinct signatures
  + Problems with this approach is that new attack patterns must continually be added to the IDPS’s database of signatures
    - Slow, methodical attack involving multiple events might escape detection.
* If signature is known then it’s easy to find out what happened and what to do

IDPSs Detection Methods (2 of 4)

* Anomaly-based detection (or behaviour-based detection)
  + Anomaly- based detection collects statistical summaries by observing traffic known to be normal
  + When measured activity is outside the baseline parameters or clipping level, IDPS sends an alert to the administrator
  + IDPS can detect new types of attacks
  + Requires much more overhead and processing capacity than signature-based detection
  + May generate many false positives

IDPSs Detection Methods (3 of 4)

* Stateful protocol analysis
  + SPA: process of comparing known normal/benign protocol profiles against observed traffic
  + Stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses; allows IDPS to better detect specialized, multisession attacks
  + Drawbacks: analytical complexity, heavy processing overhead, may fail to detect intrusion unless protocol violates fundamental behaviour, may interfere with normal operations of the protocol

IDPSs Detection Methods (4 of 4)

* Log file monitors
  + Log file monitor (LFM) is like NIDPS
  + Reviews log files generated by servers, network devices, and even other IDPSs for patterns and signatures
  + Patterns that signify an attack may be much easier to identify when the entire network and its systems are viewed as a whole
  + Requires considerable resources since it involves the collection, movement, storage, and analysis of large quantities of log data.

IDPS Response Behavior (1 of 2)

* IDPS response to external stimulation depends on the configuration and function; many response options are available
* IDPS responses can be classified as active or passive
  + Active response: Collecting additional information about the intrusion, modifying the network environment, and acting against the intrusion.
  + Passive response: setting off alarms or notifications, and collecting passive data through SNMP traps.

IDPS Response Behavior (2 of 2)

* Many IDPSs can generate routine reports and other detailed documents
* Failsafe features protect an IDPS from being circumvented.

Selecting IDPS approaches and products (1 of 2)

* Technical and policy considerations
  + What is your systems environment?
  + What are your security goals and objectives?
  + What is your existing security policy?
* Organizational requirements and constraints
  + What requirements are levied from outside the organization?
  + What are your organization’s resource constraints?
* Universities must be open to different type of applications
  + In terms of intruders

Selecting IDPS approaches and products (2 of 2)

* IDPSs product features and quality
  + Is the product sufficiently scalable for your environment?
  + How has the product been tested?
  + What user level of expertise is targeted by the product?
  + Is the product designed to evolve as the organization grows?
  + What are the support provisions for the product?

Strengths and Limitations of IDPSs(1 of 4)

* IDPSs perform the following functions well:
  + Monitoring and analysis of system events and user behaviours
  + Testing the security states of system configurations
  + Baselining the security state of a system and tracking changes
  + Recognizing patterns of system events corresponding to known attacks
  + Recognizing activity patterns that vary from normal activity

Strengths and Limitations of IDPSs(2 of 4)

* IDPSs perform the following functions well:
  + Managing OS audit and logging mechanisms and data they generate
  + Altering appropriate staff when attacks are detected
  + Measuring enforcement of security policies encoded in the analysis engine.
  + Providing default information on security policies
  + Allowing non-security experts to perform important security monitoring functions.

Strengths and Limitations of IDPSs (3 of 4)

* IDPSs cannot perform the following functions:
  + Compensating for weak/missing security mechanisms in protection infrastructure
  + Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load
  + Detecting new attacks or variants of existing attacks
  + Effectively responding to attacks by sophisticated attackers
  + Automatically investigating attacks without human intervention

Deployment and implementation of an IDPS (1 of 8)

* An IDPS can be implemented via one of the three basic control strategies:
  + Centralized: all IDPS control functions are implemented and managed in a central location.
  + Fully distributed: all control functions are applied at the physical location of each IDPS component.
  + Partially disturbed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks.

Centralized IDPS control (2 of 8)

A figure shows an illustration in which a rectangular box is shown. On the top of the box, a small square box is shown with a shadow image of a man inside it and labeled as, “IDS Console.” This square box is further pointed to two, in which one points to a cross mark. The cross mark is marked with five computer images. The next one from the square points to a fire shadow image. It is connected to the first cross image on the left. This fire image points to a cross that points to a cross image on the right and a fire image on the left bottom. The cross image on the right corner is pointed with a zigzag double sided arrow from the label internet. The perimeters of the box is shown with triangles. The one at the left top corner shows a man’s shadow image pointing with dotted lines to the first cross image. The second triangle shows a lens image points with dotted image to one of the computer images marked to cross image. The triangle also shows a triangle with shadow image of a man. The second cross image in the illustration points to a fire image which further points to a cross section. Three computer images are connected to this cross image. The third triangle is marked with dotted lines to this cross image. The triangle on the right top of the triangular box shows a microscope image which further points down with dotted lines to four circular plate structure. This further points down to spider net structure which finally points downwards with dotted lines to a small triangle that shows a microscope image. Below this a box, a horizontal rectangular block is shown, in which three triangles are shown. The first triangle shows an image of shadow of a man labeled as, “Network Monitoring System.” The second triangle shows an image of a lens labeled as, “Host-based Monitoring System.” The third triangle shows an image of a microscope and labeled as, “Application Monitoring System.” The overall box has the title that reads as, “Network Information Sources.” Below this a final rectangular box shows four different lines labeled differently. The first is a thick grey line labeled as, “IDS reporting links”, next to it is a black dotted line labeled as, “monitoring links.” The third line is thick grey line and a dot between it labeled as, “IDS Response Links.” The black thick line is shown at the last labeled as, “Main Network Links.”


Fully Distributed IDPS control (3 of 8)

A figure shows an illustration in which three triangles are shown one below the other. The first triangle on the top showing an image of shadow of a man pointing with dotted lines pointing to a fire image. This fire image is pointed to a cross image on the left which is connected with five computer images. The cross image is connected with a dotted line to the triangle on top. The third computer image is connected with dotted line to the second triangle that shows the image of a lens. The second triangle is pointed with an arrow to the third computer image. The fire image from first triangle is connected to another cross image on the right bottom side which is further connected to a cross image on the right and to a fire image on the left bottom. The fire image is connected a cross image that is connected to three computer images. The third triangle with an image of shadow of a man is shown. This triangle points to the fire image with an arrow and connected to the cross image with dotted lines. The third computer is connected to a small triangle with lens image with dotted lines and arrow. The cross image from the first fire image is connected to another cross image. In between this a triangle on the top with image of a microscope is pointed down to four plates and then to a spider like network and finally to a small triangle with image of a microscope. This triangle points back to spider network. The tringle on top is pointed to the cross image. The cross image is connected with a thick black line to the label internet. A block below it has three triangles with title that reads as, “network Information Sources.” The first triangle shows an image of shadow of a man labeled as, “network Monitoring System.” The second triangle shows a lens image in it labeled as, “Host-based Monitoring system.” The third triangle shows an image of a microscope. This is labeled as, “Application Monitoring System.” The last block has three symbol with labels as, “Monitoring links for black dotted lines, IDS Response links for a line with dots in grey color and main network links denoting a thick black line.”


Opposite of the above, finding any intrusion detection, very labour intensive

Partially Distributed IDPS control (4 of 8)

A figure shows an illustration with multiple networks. The first box on the top showing an image of shadow of a man is pointing with three dotted arrows pointing to two cross images and a fire image. The cross is connected with five computer images. The cross image is connected with a dotted line to the triangle on left top with man shadow image. The third computer image is connected with dotted line to the second triangle below it that shows the image of a lens. The fire image from the top box is connected to another cross image in the bottom, which is further connected to a cross image on the right and to a fire image on the left bottom. The fire image is connected a cross image that is connected to three computer images. The third triangle with an image of shadow of a man connects with the cross image. This triangle connects a box with shadow of a man above it. The third computer is connected to a small triangle with lens image with dotted lines. The cross image from the first box is connected to another cross image. In between this a triangle on the top with image of a microscope is pointed down to four plates and then to a spider like network and finally to a small triangle with image of a microscope. This triangle points to with other two triangles at the base of the network. The triangle on top is pointed to a small box with shadow man image again pointing to tringle on top at the right side. The cross image is connected with a thick black line to the label internet on the right side. The top box is also connected to internet. Another small network on the right top has the box with shadow man image pointing to two cross images. The first cross image is connected to four computer images. The first cross points with an arrow to the second cross image. The bow is connected with dotted lines to a triangle with shadow man image connected to another triangle with lens image. The cross image is marked with dotted lines to the tringle at right side. The fourth computer is connected with dotted lines to last triangle with lens. The second cross points to the label internet. The internet points to a box with shadow man image labeled as, “Main IDS Console.” The left side network is labeled as, “Subnet IDS Console.” The network on the right is labeled as, “Enterprise IDS Console.” A block below it has three triangles with title that reads as, “network Information Sources.” The first triangle shows an image of shadow of a man labeled as, “Network Monitoring System.” The second triangle shows a lens image in it labeled as, “Host-based Monitoring system.” The third triangle shows an image of a microscope. This is labeled as, “Application Monitoring System.” The last block has five labels as, “IDS Reporting Links, Monitoring Links, IDS Response Links, Main Network Links and IDS Master Reporting Links” with different lines.


Deployment and Implementation of an IDPS (5 of 8)

* IDPS deployment
  + Great care must be taken when deciding where to locate components
  + Planners must select a deployment strategy that is based on a careful analysis of the organization’s information security requirements and causes minimal impact
  + NIDPS and HIDPS can be used in tandem to cover the individual systems that connect to an organization’s network and the networks themselves.

Deployment and Implementation of an IDPS (6 of 8)

* Deploying network-based IDPSs
  + NIST recommends four locations for NIDPS sensors
    - Location 1: Behind each external firewall, in the network DMZ
    - Location 2: Outside an external firewall
    - Location 3: On major network backbones
    - Location 4: On critical subnets

A figure shows an illustration with a network. A label internet on the right top is connected to a fire image that is connected to a cross image. The line from internet to fire image is labeled as, ‘location 2” and line from fire image to cross image labeled as, “location 1.” In-between the fire and cross image, vertically an image of four plates is connected to a spider network. The cross image is connected to two fire images on top and bottom. The fire image on top is connected to cross image which further points to four computers and another three computers below. A label of the cross section is location 3. The fir image on the bottom is connected to a cross image which further points to four computers pointing to a call symbol icon on the top. The cross image at the bottom is labeled as, “Location 4.”
Network IDPS sensor locations (7 of 8)

Deployment and Implementation of an IDPS (8 of 8)

* Deploying host-based IDPSs
  + Paper implementation of HIDPSs can be a painstaking and time-consuming task
  + Deployment begins with implementing most critical system first
  + Installation continues until either all systems are installed or the organization reaches planned degree of coverage it will accept

Measuring the Effectiveness of IDPSs (1 of 2)

* IDPSs are evaluated using four dominant metrics:
  + Thresholds, backlists and whitelists, alert settings, and code viewing and editing
  + Evaluation of IDPS might read: at 100 Mb/s, IDPS was able to detect 97 percent of directed attacks
  + Because developing this collection can be tedious, most IDPS vendors provide testing mechanisms to verify that the systems are performing as expected.

Measuring the Effectiveness of IDPSs (2 of 2)

* Some of these testing processes will enable the administrator to:
  + Record and retransmit packets from real virus or worm scan
  + Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
  + Conduct a real virus or worm scan against a hardened or sacrificial system
* Testing process should be as realistic as possible.

Honeypots, Honeynets, and padded Cell Systems (1 of 4)

* Honeypots: decoy systems designed to lure potential attackers away from critical systems
* Honeynets: several honeypots connected on a network segment.
* Honeypots are designed to:
  + Divert an attacker from accessing critical systems
  + Collect information about the attacker’s activity
  + Encourage the attacker to stay on a system long enough for administrators to document the event and perhaps respond.

Honeypots, Honeynets, and padded Cell Systems (2 of 4)

* Padded cell system: protected honeypot that cannot be easily compromised
* In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS
* When the IDPS detects the attackers, padded cell system seamlessly transfers them to a special simulated environment where they can cause no harm – hence the name padded cell

Honeypots, Honeynets, and padded Cell Systems (3 of 4)

* Advantages
  + Attackers can be diverted to targets they cannot damage
  + Administrators have time to decide how to respond to an attacker
  + Attacker’s actions can easily and more extensively monitored, and records can be used to refine threat models and improve system protections.
  + Honeypots may be effective at catching insiders who are snooping around a network

Honeypots, Honeynets, and padded Cell Systems (4 of 4)

* Disadvantages
  + Legal implications of using such devices are not well understood
  + Honeypots and padded cells have not yet been shown to be generally useful security technologies
  + An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization’s system
  + Administrators and security managers need a high level of expertise to use these systems

Trap-and-Trace Systems

* Use a combination of techniques to detect an intrusion and trace it back to its source
* Trap usually consists of a honeypot or a padded cell and alarm
* Legal drawbacks to trap and trace
  + Enticement: act of attracting attention to a system by placing tantalizing information in key locations
  + Entrapment: act of luring an individual into committing a crime to get a conviction
  + Enticement is legal and ethical, entrapment is not.

Active Intrusion Prevention

* Some organizations implement active countermeasures
* One tool takes up unused IP address space to pretend to be a computer and allow attackers to complete a connection request, but then holds connection open.

Scanning and Analysis Tools (1 of 2)

* Scanning tools typically are used to collect information that an attacker needs to launch a successful attack
* Attack protocol is a logical sequence of steps or processes used by an attacker to launch an attack against a target system or network
* Footprinting: process of collecting publicly available information about a potential target.

Scanning and Analysis Tools (2 of 2)

* Fingerprinting: systematic survey of target organization’s internet addresses collected during the Footprinting phase to identify network services offered by hosts in that range.
* Fingerprinting reveals useful information about the internal structure and nature of the target system or network to be attacked.
* These tools are valuable to the network defender since they can quickly pinpoint the parts of systems or network that need a prompt repair to close vulnerabilities.

Port Scanners

* Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information
* Can either perform generic scans or those for specific types of computers, protocols, or resources
* The more specific the scanner is, the more useful its information is to attackers and defenders

**Firewall Analysis tools**

* Several tools automate remote discovery of firewall rules and assist administrator/attacker in analyzing them.
* Administrators who feel wary of using the same tools that attackers use should remember:
  + User intent dictates how gathered information will be used
  + To defend a computer or network well, administrators must understand ways it can be attacked
* A tool that can help close an open or poorly configured firewall will help the network defender minimize risk from attack.

**Vulnerability Scanners**

* Examine networks for detailed information and initiate traffic to determine security holes
* Listen on network and find problems with the server and client software

**Packet Sniffers**

* Captures copies of packets from network and analyses them
* Diagnosing and resolving networking issues
* In the wrong hands, can be used to eavesdrop on network traffic
* To use this legally, must be under direct authorization of owners of the network and have knowledge and consent of the content’s creators.

# SESSION 9: Physical Security

Introduction (1 of 3)

* Physical security involves the protection of physical items, objects, or areas from unauthorized access and misuse
* Most technology-based controls can be circumvented if an attacker gains physical access
* Physical security is an important as logical security

Introduction (2 of 3)

* Donn B. Parker seven major sources of physical loss:
* Extreme temperature: heat, cold
* Gases: war gases, commercial vapors, humid or dry air, suspended particles
* Liquids: water, chemicals
* Living organisms: viruses, bacteria, people, animals, insects
* Projectiles: tangible objects in motion, powered objects
* Movement: collapse, shearing, shaking, vibration, liquefaction, flow waves, separation, slide

Introduction (3 of 3)

* Energy anomalies: electrical surge or failure, magnetism, static electricity, aging circuitry; radiation: sound, light, radio, microwave, electromagnetic, atomic
* Community roles:
* General management: responsible for facility security
* IT management and professionals: responsible for environmental and access security
* Information security management and professionals: perform risk assessments and implementation reviews

Physical access control

* Secure facility: physical location with controls implemented to minimize the risk of attacks from physical threats.
* Secure facility can take advantage of natural terrain, local traffic flow, and surrounding development and can complement these with protection mechanisms (fences, gates, walls, guards, alarms).

Physical security controls (1 of 9)

* Walls, fencing, and gates
* Guards
* Dogs
* ID cards and badges
* Locks and keys
* Mantraps
* Electronic monitoring
* Alarms and alarm systems
* Computer rooms and wiring closets
* Interior walls and doors

Physical security controls (2 of 9)

* Walls, fencing, and gates
  + Some of the oldest and most reliable elements of physical security; the essential starting point for perimeter control
* Guards
  + Can evaluate each situation as it arises to make reasoned responses; most have standard operating procedures (let in or let out, they are given specific instructions)
* Dogs
  + Keen sense of smell and hearing can detect intrusions that human guards cannot

Physical security controls (3 of 9)

* ID cards and badges
  + ID card is typically concealed and name badge is visible
  + Serve as a simple form of biometrics (facial recognition)
  + Should not be the only means of control as cards can be easily duplicated, stolen, and modified
  + Tailgating occurs when an authorized individual opens a door and other people also enter

Physical security controls (4 of 9)

* Locks and keys
  + Two types of locks: mechanical and electromechanical
  + Locks can also be divided into four categories: manual, programmable, electronic, biometric
  + Locks fail and alternative procedures for controlling access must be put in place
  + Locks fail in one of two ways:
    - Fail-safe lock
    - Fail-secure lock

Physical security controls (5 of 9)

* Mantraps
  + Small enclosure that has an entry point and a different exit point.
  + Individual enters mantrap, requests access, and, if verified, can exit mantrap into facility.
  + Individual denied entry is not allowed to exit until the security official overrides automatic locks of the enclosure.

Physical security controls (6 of 9)

* Electronic monitoring
  + Equipment can record events in areas where other types of physical controls are impractical
  + May use cameras with video recorders; includes closed-circuit television (CCT) systems
  + Drawbacks
    - Passive; does not prevent access or prohibited activity
    - Recordings often are not monitored in real time; must be reviewed to have any value

Physical security controls (7 of 9)

* Alarms and alarm systems
  + Alarm systems notify people/systems when an event occurs
  + Detect fire, intrusion, environmental disturbance, or an interruption in services
  + Rely on sensors that detect an event, for example, motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors

Physical security controls (8 of 9)

* Computer rooms and wiring closets
  + Require special attention to ensure confidentiality, integrity, and availability of information.
  + Logical access controls are easily defeated if attacker gains physical access to computing equipment.
  + Custodial staff, often the least scrutinized people who have access to offices, are given greatest degree of unsupervised access.
  + Should be installed with motion detectors

Physical security controls (9 of 9)

* Interior walls and doors
  + Information asset security is sometimes compromised by improper construction of facility walls and doors.
  + Facility walls are typically either standard interior or firewall.
  + High-security areas must have firewall-grade walls to provide physical security against potential intruders and fires.
  + Doors allowing access to high-security rooms should be evaluated.
  + To secure doors, install push or crash bars on computer rooms and closets.

Fire Security and Safety

* Most serious threat to safety of people who work in an organization is fire.
* Fires account for more property damage, personal injury, and death than any other threat.
* It is imperative that physical security plans implement strong measures to detect and respond to fires and fire hazards.
* High temp, material to burn, and oxygen

Fire detection and response (1 of 4)

* Most serious threat to safety of people who work in an organization is fire.
* Fires account for more property damage, personal injury, and death than any other threat.
* Flame point: temperature of ignition
* Deny an environment of temperature, fuel or oxygen
  + Water and water mist systems
  + Carbon dioxide systems
  + Soda acid systems
  + Gas-based systems

Fire detection and response (2 of 4)

* Fire detection
  + Fire detection systems fall into two general categories: manual and automatic
  + To prevent an attacker slipping into offices during an evacuation, programs often designate a person from each office area to serve as a floor monitor
  + There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection

Fire detection and response (3 of 4)

* Fire suppression
  + Systems can consist of portable, manual, or automatic apparatus
  + Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D, Class K
  + Installed systems apply suppressive agents, usually either sprinkler or gaseous systems
  + When you put water on oil it changes into vapor
  + Class A – fire at home (paper, carton , timber)
  + Class B – liquid, petrol on fire
  + Class C – If given device is connected to electricity
    - If water is composed to it, it can conduct electricity (A on B)

Fire detection and response (4 of 4)

* Gaseous emission systems
  + Until recently, two types of systems: carbon dioxide and Halon
  + Carbon dioxide removes fire’s oxygen supply
  + Halon is clean but has been classified as an ozone-depleting substance; new installations are prohibited
  + Alternative clean agents presented are reported to be less effective than Halon
    - See Table 9-1 in the textbook

Gaseous fire suppression system (1 of 2)

* System Components:
* Discharge nozzles
* Piping
* Control panel
* Discharge or warning alarms (s)
* Hazard warning or caution signs
* Automatic fire detection devices (s)
* Manual discharge station (s)
* Storage container (s) and extinguishing agent

Gaseous fire suppression system (2 of 2)

An illustration shows a room like structure shown in side view. A door is shown and is numbered as, 5 with a notice “Warning” and a triangle is shown below it in the front view of room. A rectangular box like structure is numbered as, 4 and is shown to the left of the door. Many cylindrical structures numbered as, 8 are shown on the side wall with many pipes attached to it. Many pipes with nozzle numbered as, 1 and a big nozzle in the center of room and is labeled as, 6 at the bottom is shown on the top view of room. A pipe near the front view of room is numbered as, 2. An “Exit” door is shown at the back side of room. A box like structure is shown to the right of door and is numbered as, 7. A box is shown on the top of back wall and is numbered as, 4. A box is shown on the side wall beside the cylinder and many pipes emerges from the box and is numbered as, 3. The text to the left of the room reads as, “1 Discharge nozzles, 2 Piping, 3 Control panel, 4 Discharge or warning alarm(s), 5 Hazard warning or caution signs, 6 Automatic fire detection device(s), 7 Manual discharge station(s), 8 Storage container(s) & extinguishing agent.”


Failure of Supporting Utilities and Structural Collapse

* Supporting utilities (heating, ventilation, and air conditioning; power; water) have significant impact on continued safe operation of a facility.
* Each utility must be properly managed to prevent potential damage to information and information systems.
* Earthquakes and house stability

Heating, Ventilation, and Air Conditioning (1 of 5)

* Areas within heating, ventilation, and air conditioning (HVAC) systems that can cause damage to information systems include:
  + Temperature
  + Filtration
  + Humidity
  + Static electricity

Heating, Ventilation, and Air Conditioning (2 of 5)

* Ventilation shafts
  + While ductwork is small in residential buildings, in large commercial buildings, it can be large enough for an individual to climb through
  + If ducts are large, security can install wire mesh grids at various points to compartmentalize the runs
* Power management and conditioning
  + Power systems used by information-processing equipment must be properly installed and correctly grounded

Heating, Ventilation, and Air Conditioning (3 of 5)

* Noise that interferes with the normal 50-Hertz cycle can result in inaccurate time clocks or unreliable internal clocks inside the CPU
* Grounding and amperage
  + Grounding ensures that the returning flow of current is properly discharged to ground
  + Ground fault circuit interruption (GFIC) capable of quickly identifying and interrupting a ground fault
  + Overloading a circuit can create a load exceeding electrical cable’s rating, increasing the risk of overheating and fire

Heating, Ventilation, and Air Conditioning (4 of 5)

* Uninterruptible power supply (UPS)
  + In case of power outage, UPS is the backup power source for major computing systems
  + Basic UPS configurations:
    - Standby
    - Line-interactive
    - Standby online hybrid
    - Standby Ferro resonant
    - Double conversion online
    - Data conversion online

# SESSION 10: Physical Security

**Definition of Digital forensics**

* **Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime

**Steps in a digital forensic examination**

* Acquire evidence
* Analyse evidence
* Produce report
  + Provide ‘expert’ consultation and testimony

**Acquisition**

* Search Warrant & search order (Anton Piller) orders
  + Execution is same
  + Search warrant is issued by high court judge
* Delivered to the Lab
* On site
* Overt and covert

**What are we “Acquiring”**

* Digital information that is accessible from:-
  + Hard Drives, (PCs, Laptops, Servers, Tablet computers)
  + USB sticks
  + Mobile Phones
  + Cameras
  + CDs , DVDs, Tapes…..and anything else.

**A Copy and a Clone/Forensic image**

* Operating system will look at all records which are in logical structure on the disk and copy that
* We can launch specific software which will wipe out empty space
* A forensic image has digital signatures
* Can be used in court as “best” digital evidence

**Acquisition process**

* Digitally photograph evidence items
* Formally document evidence items
* Acquire evidence item onto ‘sterile drive’
  + We need this in order to download
* Verify ‘Digital Signature’ of acquisition

**Specialized Hardware and Software**

* ‘Encase’ ‘FTK Imager’
* Write Blocking hardware to ensure that the subject item is not written to – i.e original evidence corrupted
* FTK – index’s whole file, simply searches the index and provides the answer very quickly
* If you have simple cases encase is better, but for complex cases FTK is better. But the whole record needs to be indexed.

**Analysis (Searching)**

* What are we looking for:
  + Documents
  + Emails
  + Pictures
  + Who was on the system and when
  + Who copied what off the system and when
  + Anything else

**Search warrant**

**High priorities from judges in issuing warrants:**

* Scope of the warrant – must be clearly defined
* Legal privilege issues
* Impact on the running of the business
* Our report must only refer to the case in the search warrant
* If we do a search, and we take evidence then the company may not operate until you download the data.
  + E.g. company loses money, you found nothing so who will pay for it

**An Expert Witness**

* Must have read agreed to the high court code of conduct for Expert Witnesses
* May gave an “Opinion” in evidence
* Is there to assist the court. Does not act as an advocate for prosecution or defence
* They are allowed to formulate this opinion, this opinion must only state the facts and not be bias.

**Search warrants – a very modern problem**

* The history of search warrants is linked to physical premises
* Data might not be in particular location, search warrant will not evaluate all the offices and not bring any results.

A matter of scale

* The manual search may involve the searching of 20 filing cabinets and the removal of one filing cabinets worth of documents
* The computer forensic consultant might remove information equivalent to 10,000 filing cabinets without searching to see if any of it is relevant (or privileged).

Safe guards the court is looking for

* Independent digital forensic consultant
* Personal undertakings to the court regarding actions
* To be aware of the impact of the business
* To hold information, remove from plaintiff
* As an expert witness to act on behalf of the court (as per the undertakings re an expert witness)

Qualifications, training, experience and ethics

* Must have:
  + Formal qualifications (degrees)
  + Training certificates encase and FTK
  + Wide and detailed experience in IT industry
  + Legal procedure understanding
  + Business experience
  + Personal integrity
  + Credibility as an expert witness (professional indemnity insurance)

Future trends

* Larger storage devices
* More information
* More mobile data
* The cloud
* Evolving legal issues – case law

# SESSION 11: Security and Personnel

Introduction

* When implementing information security, there are many human resource issues that must be addressed.
  + Positioning and naming the security function
  + Staffing for or adjustments to the staffing plan
  + Assessing the impact of information security on every IT function
  + Integrating solid information security concepts into personnel management practices
* Employees often feel threatened when an information security program is being created or enhanced.

Positioning and Staffing the security function

* The security function can be placed within:
  + IT function
  + Physical security function
  + Administrative services function
  + Insurance and risk management function
  + Legal department
* IS should balance duty to monitor compliance with needs for education, training, awareness, and customer service.

Staffing the information Security function (1 of 6)

* Selecting personnel is based on several criteria, including some not within the control of the organization (supply and demand)
* Many professionals enter security market by gaining skills, experience, and credentials.
* At present, the information security industry is in a period of high demand.

Staffing the information Security function (2 of 6)

* Qualifications and requirements
  + Establishing better hiring practices requires the following:
    - General management should learn more about skills and qualifications for positions
    - Upper management should learn about the budgetary needs of information security function
    - IT and general management should grant appropriate levels of influence and prestige to information security
  + Organizations typically look for a technically qualified information security generalist

Staffing the information Security function (3 of 6)

* Qualifications and requirements
  + Organizations look for candidates who understand:
    - How an organization operates at all levels
    - Information security is usually a management problem, not a technical problem
    - Importance of strong communications and writing skills
    - The role of policy in guiding security efforts
    - Most mainstream IT technologies

Staffing the information Security function (4 of 6)

* The terminology of IT and information security
* Threats facing an organization and how they can become attacks
* How to protect an organization’s assets from information security attacks
* How business solutions can be applied to solve specific information security problems

Staffing the information Security function (5 of 6)

* Entry into the information security profession
  + Traditionally, many IS professionals entered the field through one of two career paths:
    - Law enforcement or military
    - Technical IT professional, working on security applications and processes
  + Today, students tailor degree programs to prepare for work in IS
  + Orgs, foster greater professionalism by matching qualified candidates to clearly defined roles in IS

Staffing the information Security function (6 of 6)

* Information security positions
  + Use of standard job descriptions can increase the degree of professionalism and improve the consistency of roles and responsibilities between organizations

Information security positions (1 of 4)

* Chief information security officer (CISO)
  + Top information security office; frequently reports to chief information officer
  + Managers the overall information security program
  + Drafts or approves information security policies
  + Works with CIO on strategic plans
  + Develops information security budgets
  + Sets priorities for purchase/implementation of information security projects and technology
  + Makes recruiting, hiring and firing decisions or recommendations
  + Acts as spokesperson for information security team

Information security positions (2 of 4)

* Chief security officer (CSO)
  + CISO’s position may be combined with physical security responsibilities
  + Knowledgeable in both IS requirements and “guards, gates, and guns” approach to security
* Security manager
  + Accountable for day-to-day operation of information security program

Information security positions (3 of 4)

* Accomplishes objectives as identified by CISO, resolves issues identified by technicians
  + Typical qualifications: often have accreditation; ability to draft middle – and lower-level policies, standards, and guidelines; budgeting, project management, and hiring and firing; ability to manage technicians
* Security technician
  + Technically qualified employees tasked to configure security hardware and software
  + Tend to be specialized

Information security positions (4 of 4)

* Typical qualifications:
  + Prefer experts, certified proficient technical
  + Some experience with software’s and hardware’s

Credentials for Information security professionals

* Many organizations seek industry-recognized certifications
* Most existing certifications are relatively new and not fully understood by hiring organizations.

Certifications (1 of 4)

* A book of knowledge which you need to acquire
  + ISC certifications
  + CISSP (certified information systems security professional)

Certifications (2 of 4)

* Systems security certified practitioner
* Certified secure software
* …

Certifications (3 of 4)

* ISACA
  + More about management certificates

Certifications (4 of 4)

Advice for information security professionals

* Always remember: business before technology
* Technology provides elegant solutions for some problems, but only exacerbates others.
* Never lose sight of goal: protection.
* Be heard and not seen
* Know more than you say; be more skillful than you let on.
* Speak to users, not at them
* Your education is never complete.

Employment Policies and Practices

* An organization should make information security a documented part of every employee’s job description
* Management community of interest should integrate solid concepts for information security into the organization’s employment policies and practices.
* From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls.
* The CISO and information security manager should work with human resources department to incorporate information security into guidelines used for hiring all personnel

Job Descriptions

* Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions.
* An organization should avoid revealing access privileges to prospective employees when advertising open positions

Advice for information security professionals

* Always remember: business before technology

Interviews

* An opening within the information security department creates a unique opportunity for the security manager to educate HR on certifications, experience, and qualifications of a good candidate
* Limit information provided to the candidate on the responsibilities and access rights of the new hire.
* Important to exercise caution when showing candidate around facility.

Background Checks (1 of 2)

* Investigation into a candidates’ past should be conducted before organization extends offer to a candidate
* Background check differ in the level of detail and depth with which a candidate is examined
* Not allowed to right a bad remark from previous organization.

Background checks (2 of 2)

* May include:
  + Identity check
  + Education and credential check
  + Previous employment verification
  + References check
  + Worker’s compensation history
  + Motor vehicle records
  + Drug history
  + Credit history and more

Employment contracts

* Once a candidate has accepted a job offer, employment contract becomes an important security instrument
* Many security policies require an employee to agree in writing to monitoring and nondisclosure agreements
* Policies governing employee Behaviour may be classified as “employment continent upon agreement”, whereby employee must agree to conform with the policies before.

New hire orientation

* New employees should receive extensive information security briefing on policies, procedures, and requirements for information security
* Levels of authorized access should be outlined
* By the time employees start, they should be briefed on security component’s

On-the-job Security training

* An organization should integrate security awareness education into job orientation and security training
* Keeping security at the forefront of employee’s minds helps minimize their mistakes and is an important part of information security awareness mission
* External and internal seminars should also be used to increase security awareness for all employees, particularly security employees.

Evaluating Performance

* Organizations should incorporate information security components into employee performance evaluation
* Employees pay close attention to job performance evaluations
  + Are more likely to take information security seriously if violations are documented in them

Termination (1 of 4)

* When employee leaves an organization, security related issues arise
* Key issues is continuity of protection of all information to which the employee had access
* After having delivered keys. Keycards and other business property
* Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback.

Termination (2 of 4)

* Hostile departures include termination for cause, permanent downsizing, temporary layoffs, or some instances of quitting
  + Before the employee is aware, all logical and keycard access is termination
  + Employee collects all belongings and surrenders all keys, keycards, and other company property
  + Employee is then escorted out of the building.

Termination (3 of 4)

* Friendly departures include resignation, retirement, promotion, or relocation.
  + Employee may be notified well in advance of departure date
  + More difficult for the security to maintain positive control over the employee’s access and information usage
  + Employee accounts usually continue with new expiration date
  + Employees come and go at will, collect their own belongings, and leave on their own.

Termination (4 of 4)

* Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
* Possible that employees foresee departure well in advance and being collecting organizational information for their future employment
* Only by scrutinizing system logs after the employee has departed can the organization determine if there has been a breach of policy or a loss of information
* If information has been illegally copied or stolen, report an incident and follow the appropriate policy.

Security considerations for temporary employees, consultants, and other

workers.

* Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
* Relationships with these individuals should be carefully managed to prevent possible information leak or theft.

Contract Employees

* Typically hired to perform specific services for organization.
* Host company often makes contract with a parent organization rather than with an individual for a task
* In a secure facility, all contract employees are escorted from room to room, as well as into and out of facility.
* There is need for restrictions or requirements to be negotiated into contract agreements when they are activated.

Internal control strategies (1 of 4)

* Separation of duties is a cornerstone in the protection of information assets and the prevention of financial loss.
  + Used to reduce chances that an employee will violate information security; stipulates that completion of significant task requires at least two people
* Two-man control: two individuals review and approve each other’s work before the task is categorized as finished.

Internal control strategies (2 of 4)

* Job rotation: employees know each other’s job skills
  + Ensures no one employee performs actions that cannot by physically audited by another employee
* Garden leave used by some companies to restrict the flow of proprietary information when an employee leaves to join a competitor.
  + Garden leave is when someone plans to resign from a company when they are in position of some important situation.

Privacy and the security of personnel data

* Organizations required by law to protect sensitive or personal employee information
* Includes employee addresses, phone numbers, social security numbers, medical conditions, and family names and addresses
* Information security groups should ensure these data receive at least the same level of protection as other important organization data.

# SESSION 12: Handling Cyber Warfare

**War definition**

War is a state of armed conflict between societies. It is generally characterized by extreme aggression, destruction, and mortality, using regular or irregular military forces.

**Cyber war vs cyber terrorism**

* The same tools
* Difference in motivation
* Slightly different targets

**Cyber war**

* Conflict in which digital technology plays important role
  + Cyber war could be “total” – digital technology is the only tool used
  + Digital technology may be a source o collateral damages along with the other technology used.

**Moonlight Maze**

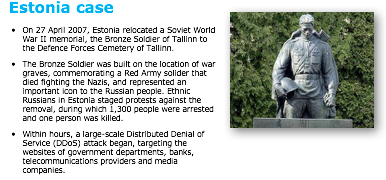
* Moonlight maze was the codename assigned to a series of attacks against The Pentagon, NASA, United States Department of Energy and a range of research organisations that were identified in March 1998.
* The USA department of defence traced the attacks back to the Russian academy of science.
* As a result of Moonlight Maze, the Clinton Administration created the National Incident Protection Center as an inter-agency body tasked to protect the United states critical infrastructure from cyber-attack.

**Titan Rain**

* The events of Moonlight Maze were repeated a few years later, as again United States military systems were targeted in a series of raids.
* The attacks were first seen in 2003 at Lockhead Martin, a US military contractor, and later at Sandia National Laboratories, a subsidiary of Lockheed martin.
* The attacks were believed to be carried out by government – supposed cells in China. China denied that the attacks came from Chine, and argued that the attacks had been relayed through Chinese computers, but had not originated in China.

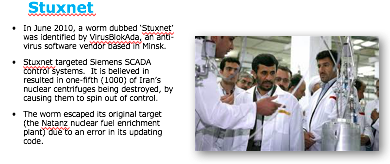
**Pentagon network under attack**

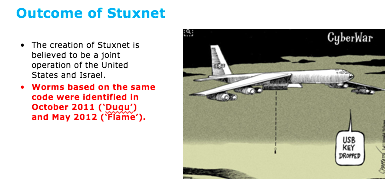
In 2006, Major General William Lord, Director of Information, Services and Integration in the United States Air Force’s Office of warfighting integration stated that China has downloaded 10 to 20 terabytes of data from the NIPRNet.



**Outcome of Estonia case**

* The attack on Estonia highlighted the cyber warfare risk to NATO, and placed, the enhancement of cyber capabilities near the top of NATO’s agenda.







**Attacks against refineries**

* 30,000 computers at Saudi Armco, the state owned Saudi Arabian Oil company, were crippled as result of a virus dubbed Shamoon. At the same time, workstations at Qatar’s RasGas, a large liquetied natural gas operation.
* USA believed Ira was behind the attacks on the refineries. Iran defined any involvement