**The CIA Triad**Threat is an event that can cause negative impact to an organization. So CIA is angle to avoid it. **Confidentiality** a set of rules that limits access to information. ***Integrity*** the ***assurance*** that the information is ***trustworthy and accurate. Availability*** a guarantee of reliable access to the information by authorized people.

Malware. ***Virus***: replicates by attaching to some executable files; aims to modify files or damage systems ***Worm***: similar to virus, with the additional "strength" that is can survive and replicate on its own without the need to attach to something else| **Characteristics**: Self-replicating and exploring |May carry other payload |Causing congestion |May carry good intention |Taking actions without consent. Trojan ***Horse***: disguises its real purpose and is installed by users inadvertently **Ransomware**: a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid Which one of three doesn’t replicate itself? ***Trojan*** Which one can clog the Internet? ***Worm Which*** one(s) must “live off” other legitimate files? ***Virus and Trojan Which*** one spreads the fastest? ***Worm* Countermeasure:** Update OS and patches |Install antivirus software| don't download files from an untrusted network or website| Make sure your browser's set to request your permission before running pop-ups, files, or programs from the internet.| Don't open files from people you don't know, or files from people who may not have a reason to message you directly| Regular backups of critical data must be made and stored on preferably read-only media such as CDs and DVDs.| Scan external storage devices on an isolated machine .**Communication Interception.*****Packet Sniffer***: Packet Sniffing is a technique of monitoring every packet that crosses the network***IP Spoofing***: Modifies source address to spoof firewall.***Pharming***: Attackers use malware to change host file or perpetrate DNS Cache Poisonings. Even Victim type correct URL. still go to wrong website and provides sensitive data to attackers.***Man-in-the-Middle Attack***: Attacker places him/herself in the middle of communication between two targets: −e.g., by compromising the network routers in either/both targets’ networks −May relay, modify, or even block communication contents entirely Which one is the hardest to detect but easiest to defend against? ***Sniffing*** **Countermeasure:** firewall| intrusion detection system| prevent malware be installed **Social Engineering:** Phishing Emails: Fake EmailPhishing Emails: Fake Email Vishing : Fake Voice These are Social Engineering : The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes **Countermeasure:** Conduct regular phishing awareness programs and simulation for all staff| Maintain a principle of least privilege for each user group and account.| Remove or disable commonly abused and non-essential services, if appropriate. ***Software Flaw******SQL Injection*** :When developers fail to properly validate user input before using it to query a relational database, one may gain access to unauthorized information***Buffer Overflow***: A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions. Assembly and C/C++ more danger since direct access to memory .**Countermeasures**: hire better IT team| Increase IT budget **Service Disruption *DoS***: disrupts service provision and so business continuity by making a server “busy” by send thousands of false requests to “flood” a server so that it cannot respond to other legitimate users| Common Dos: SYN Flooding exploits TCP three-way handshake feature to establish connections.1.Malicious client not sending ACK back to server.2. SYN request started by a spoofed IP address***Distributed DoS (DDoS)***: More sophisticated attacks involve distributed zombies, hence the name DDoS **Countermeasures** Largely technical/Work with reliable cloud service providers, ISP, and police **Others: Password Cracking**1. Guessing - Birthday, Id, Name, etc 2. Dictionary attack – repeatedly try dictionary words until access is granted3. Brute-force attack - all combinations 4. Rainbow table - a precomputed table for reversing cryptographic hash function, usually for cracking password hashes. Tables are usually used in recovering a password up to certain length consisting of a limited set of characters. **Countermeasures: better password with multiple factor**

***Sabotage or Vandalism***:Involve deliberate sabotage of a computer system or acts of vandalism to destroy an asset or damage the image of an organization. ***IoT and IIoT***:These are the systems in which failure often results in life-threatening or other emergency situations. ***Cryptojacking*** : Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. **CIA Mapping: Malware**CIA**SQL**CI\***Buffer**IA**Sniffer**C**Spoofing**C**Pharming**CI\***Man**CIA**DDOS**A**Phishing**CIA**Password**CI\***IOT**CIA\***CrypoJacking:**A\***Prmopt**C\***Sabotage/Vandalism**IA**SupplyChain**C\*I\***AI**CI\* **Authentication method (access control)**Something you know-Password, security questions| Something you have-Token, SMS, ID card| Something you are or can produce-Signature, retina scan, facial recognition, voice **Firewall** A specific type of computing facility to control network traffic, and keep your organization’s internal network (or other devices, data, applications, etc.) safe from outside threats| **Regulates all inbound traffics, outbound traffics| Can be implemented as hardware or software.** Does encrypted traffic affect how firewall works? – no How many rules do you think there will be? –from a few hundreds to a few thousands and even more, depending on the size of the organization 3.Will inbound rules be different from outbound rules? – yes What should be the last rule? –deny all Subject to what type of attack? –spoofing attack  
**Common Port:7Echo|20FTP|21FTP|23Telent|25SMTP|53DNS|80HTTP|110POP3  
Honeypots:** decoy systems designed to lure potential attackers away from critical systems

**Honeynets**: several honeypots connected together on a network segment| **For**: Divert an attacker from accessing critical systems| Collect info. About the attacker’s activity| Encourage attack stay logger| document the event and respond| **Issues**: Legal implications unclear| Attacker will fight back| need talent on admin  
**A diagram of a firewall

Description automatically generatedArchitecture** Single Bastion Hosts |Dual-homed Bastion Host|Screened Subnet **A diagram of a computer network

Description automatically generatedA diagram of a computer network

Description automatically generated**A diagram of a firewall

Description automatically generated

Screened Subnet with DMZ (Demilitarized Zone)  
A diagram of a network

Description automatically generated**A diagram of a system interconnection model

Description automatically generated**A blue and white sign with black text

Description automatically generated**A blue and white box with red text

Description automatically generated**

**Type of Firewall 1.Mac Layer Firewall |Packet Filtering Firewalls:** UDP and TCP header itself has some information about the src port and Dst port Most basic form of firewall protection| **Accept/reject data packets based on the packets’ header information :Source and destination IP addresses via an access control list (ACL) (i.e., firewall rule set)|Efficient and low cost as it only examines header information of packets| No concept of “state” of packets, which makes it less secure| Has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection or is just a rogue packet | Stateful Firewall (Dynamic Packet Filtering)** Keep track of connection status using a state table and a firewall ruleset: |**Accept traffic from the outside that matches an existing entry in the dynamic state table |Could be slower than packet filtering firewall| Far more secure than packet filtering firewall| Additional processing cost in order to maintain the state table|** **Application Layer (Proxy) Firewall Sits between the internal network and the outside servers and gateways; serves as an intermediary that allows two systems to communicate indirectly; Hides internal network configuration| Typically installed in a dedicated computer separate from the filtering router| Allow or deny incoming traffic related to applications or services, such as web or FTP|** **Checks IPs; validates TCP handshakes; deep packet and stateful inspections; audit and logging; user authentication IDPS** Checks IPs; validates TCP handshakes; deep packet and stateful inspections; audit and logging; user authentication: Differences Between Firewall and IDPS **Firewall:** examine header| Sit at perimeter of network| Block packets by ip/port| Rule-based| like a door man| easier to implement| more complex configuration| **IDPS** examine header and payload | site between firewall and trust network | Analyse packets, signal alarm and(drop, alert, or clean) | Rule-based or anomaly-based| Like detective| Detection Methods Signature-based –match traffic or data patterns with pre-defined or known attack (suspicious) patterns(more alarms)| Statistical anomaly-based –sample network activities and compare them with “normal” baselines IDS Mode Passive Analyse and report the information/problem (i.e., generate alarms) that it has collected| Does not interfere with the traffic itself | Wait for administrator’s actions **Active** Aautomatically initiate responses when alerts are triggered e.g., collect and archive additional information, modify the environment, take action against the intruders, etc. What if the traffic is encrypted? –greatly affects the IDPS’s ability to identify malware What if there is heavy network traffic? –IDPS can cause network congestion and negatively impact the network’s performance: **VPN**: Extends an organization’s internal network to remote locations| Provide private and secure network connection between systems| VPN must accomplish (CIA): **C:** the carrier network will route the data, but unable to decrypt it (through encryption).**I:** messages transported across the network cannot be changed easily while they are in transport (through encapsulation).**A:** users from both ends need to authenticate themselves, to be able to use the network (through passwords, keys, digital signatures, etc.) **Mode:** Tunnel Establishes two perimeter tunnel servers to encrypt all traffic that will traverse an unsecured network Entire client package encrypted and added as data portion of a packet from one tunnelling server to another Transport Data within IP packet are encrypted, but header information is not| Allows user to establish secure link directly with remote host, encrypting only data contents of packet| 1. Two popular uses: End-to-end transport of encrypted data 2. Remote access worker connects to an office network over Internet by connecting to a VPN server on the perimeter. **Cryptography**: the process to keep a message secret from unintended audiences: **Cryptanalysis**: the process to obtain original text from encrypted message without knowing the methods/keys: **Cipher Methods**: Substitution: Mono-alphabetic Substitution **How to crack: Use frequency chart to improve efficiency of decryption**  
A screen shot of a computer

Description automatically generated **Poly-alphabetic substitution**A close-up of a chart

Description automatically generatedTransposition Caesar block: fit the text to a number square Larger Size!=secure . just les eff  
A green text on a white background

Description automatically generated**Block Transposition 8bit is not enough larger better**A close up of numbers

Description automatically generated **User-generated key: The Vigenere Square** Which letter shall not be used as part of the key? –A **Exculsive Or** Use XOR with content and Key  
Encryption Algorithm and Key Size which is more important and why? - **Size** −What’s the key for each method? • For mono-alphabetic, the key is number of **key shifted** • For poly-alphabetic, the key is **dictionary** • For Caesar block, the key is **block** • For transposition, the key is Shift the values within a block of text • For the other two methods, the keys are encryption key −What do you need to pass on to the recipient in order for him or her to decipher? **Ciphered and Key  
Hash:** used to confirm the identity of a specific message and confirm that the content has not been changed| only instead generates a hash value or message digest.| Irreversible| same data; same hash, Uniqueness. Near impossible 2 message has same key(hash collision) **Collision attack :** using same hash to pretend non-malicious exe. Use case 1 password protection. The salt is typically stored right next to the salted and hashed password. Additionally, the salt should be unique per password. PWD= Hash(hash(password)+salt) Use case 2: Hash as message digest. Confirm the sender is same person. Does this process ensure confidentiality and integrity? – **Only integrity**.  
Subject to what types of attack? – **sniffing, spoofing and man-in-the-middle.  
PKI:** Why Cryptography **Confidentiality** –unauthorized people should not see the message: Who should see the information? **Integrity** –the message is not tampered with during the transmission: did anyone change the information?” **Authenticity** –verify the identity of the person who sent and receive the information**:** Who sent and who received the information? **Non-repudiation** –prevent someone from denying a transaction: Can someone deny that he/she had sent a message earlier? **Symmetric Key Implementation:**Data Encryption Standard (DES)**:** Block cipher developed by IBM; endorsed by US government in 1977| 56-bit key on 64-bit data block | 16 rounds of permutation, character substitution, and XOR operation | Brute force attack, in 1998, US$250,000 hardware 3 days   
Advanced Encryption Standard (AES): Federal Information Processing Standard (FIPS) cryptographic algorithmic for use within the US government| Key lengths of 128, 192, or 256 bits (AES-128, AES-192, and AES-256)| 9-13 rounds of operations involving substitution, transposition, XOR, and matrix multiplication **RC4** A stream cipher with a 40 to 2048-bit key. It generates a keystream by using index.| used in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) with the Hypertext Transfer Protocol over SSL (HTTPS) protocol; and WEP and WPA on wireless networks. RC5 it is a block cipher using a 1 to 255 round (12 originally suggested) Feistel-like network with 32, 64, or 128-bit blocks published in 1994. The key size is 0 to 2040 bits. Also uses modular addition and bitwise XOR. **Symmetric Key Cryptosystem:** No. of keys needed with n parties = n(n-1)/2: pros: Fast| Simple| theoretically strong if key is secure **cons** Key distribution and management| fast-> easier to break| if the key lost , the security break down. **Asymmetric encryption - Public Key Infrastructure (PKI):** Asymmetric Key System: A key pair for each person: One as a public key – open for public access, The other as private key –restricted to owner| Deriving the private key from public alone is not possible. **Public Key Cryptosystem:**  from math. Factoring a product of large prime number is extremely hard. **Public Key Infrastructure (PKI) Pros:** Easier key management and distribution| The private key is never distributed and therefore is more secure| Scalable| no published methods to defeat the system if a larger enough key is used. **Digital Certificate:** A digital certificate is an electronic document that contains a public key value and identifying information about the entity that controls the key.| Often issued by a third party, i.e., a certificate authority (CA)**.   
Protocols for secure communication:** Web SSL,TLS| Email S/MIME,PEM,PGP| Wireless WEP,WPA,WPA2,WPA3| Bluetooth passkey **SSL/TLS(HTTPS) each session has respective key PGP** Pretty Good Privacy (PGP) is a hybrid cryptosystem, available free or at low cost.| Open source for encryption and authentication of email and file storage. It uses ZIP to compress the message after it has been signed, before driving Bluetooth exploited by anyone with a range of approximately 30 feet (10 meters)| Do not accept an incoming communications pairing request unless you know the identity of the requester.| Avoid setting up pairing in public| Delete unused bluetooth connection | Disable bluetooth when not in use **Digital Forensics**  
**A white background with black text

Description automatically generated**

|  |  |  |
| --- | --- | --- |
| Risk management | | |
| Risk identification where and what is the risk – identifying assets | Risk analysis How severe is the current lv of risk- identifying vulnerabilities | Risk evaluation is the current level of risk acceptable – threat/ asset matrix(qualitative) quantitative risk assessment |
| Risk Control | | |
| Risk treatment what do I need to do to bring the risk to an acceptable lv | | |

**PKI With Digital Certificate**A diagram of a person and person working on a computer

Description automatically generated **Risk Management:**

Risk identification: How critical is the asset to the success of the organization? How much does the information asset contribute to profit generation? How expensive is the information asset to replace? How expensive is the information asset to protect? How much embarrassment or liability would the asset’s loss or compromise cause? A yellow and white rectangular box with black text

Description automatically generated  
Risk analysis: Identifying Vulnerabilities   
A diagram of a company

Description automatically generatedA diagram of a risk

Description automatically generated  
**Risk evaluation:** Threats-vulnerabilities-assets (TVA) Worksheet It is a threat to asset matrix **Risk evaluation**: Quantitative risk assessment  
**Risk treatment** : Select Control Strategies| Defense : Prevent Exploitation of the vulnerability| Countering threat, removing vulnerabilities, limiting asset access, and adding protective safeguards| Transference: shift risks to others | Hiring firms with expertise to provide security service | Mitigation : reduce the impact of the attack instead of the success of the attack : Contingency planning (CP) Incident Response (IR) Disaster recovery, Business Continuity (BC) |  
Acceptance : do notihing | valid only when function, service infom or assets does not justify the cost of protection| termination : avoid business activity that introduce uncontrollable risk| May seek an alternate mechanism to meet the customer needs. Which is the most passive strategy? Acceptance **Contingency Planning(CP)** To prepare the organization to anticipate, react to, and recover from events that threaten the security of information **NIST CP Methodology  
A diagram of a business plan

Description automatically generated** **A white background with black text

Description automatically generated**  
**Business Impact Analysis(BIA)** helps determine which business functions and information systems are the most critical to the success of the organization. **(MTD) : The maximum time a business can tolerate the absence System recovery time (RTO) : Time to recover system  
 Work recovery time (WRT) : Time to recover data/work  
Incident Detection | Incident Reaction| Disastor | Business Continuity Planning (BCP)  
A screenshot of a computer

Description automatically generated** A red and green rectangular boxes with black text

Description automatically generatedA screenshot of a computer

Description automatically generatedA white text on a white background

Description automatically generated