CYBER SECURITY

FOR CISO/CTO/CIO

CHAPTER 1
CYBERSECURITY CONCEPTS

SUBTOPICS:
Essential terminologies: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering(Social Engineering, Foot Printing & Scanning).
Open Source/ Free/ Trial Tools: nmap, zenmap, Port Scanners, Network Scanners.

NEED FOR CYBERSECURITY

With the boom of digitisation, lots of information is available online, with new resources it opens up the surface which could be attacked. It is absolutely important to protect all software and hardware from malicious attacks. To furthermore protect the privy information from transmission, modification or deletion.

WHAT IS CYBERSECURITY?

Before starting off with the concepts of cybersecurity, it is absolutely imperative for us to know what the term cybersecurity means. **Cyber Security involves securing not just the data but also the technologies used to store that data. It is the process and techniques involved in protecting confidential data, computer systems, networks and other applications from cyber attacks, i.e to protect anything in the cyber realm**. It requires an understanding

of what the information is to the company, potential information threats, such as viruses and other malicious code.

The need for cyber security rises due to a surge in the usage of computer systems and reliance on smarter devices which implement the concept of ”Internet of things”.

Cybersecurity strategies include identity management (authentication and authorization), risk management, and incident management.

Some of the cyber attacks are done to:

- Tamper with the data and the system in which they are stored.
- The exploitation of resources.
- Unauthorized access to the targeted system and accessing sensitive information.
- Disrupting the normal functioning of the business and its processes.
- Using ransomware attacks to encrypt data and extort money from victims.
- Using an affected system to launch attacks.
- To steal financial records from the user.
- To get access to computer systems of financial institutions or web sites and apps that store credit card numbers and bank account details, for manipulating markets, making illicit financial gains or selling information to the black market.

CIA TRIAD

The CIA triad are the fundamental aspects of information security. In brief **confidentiality is a set of directives to limit access to**

information, integrity is the guarantee that the information is safe and accurate and availability is an assurance that the information is within the reach of trustworthy personnels. CIA stands for :

A. Confidentiality
B. Integrity
C. Availability

CONFIDENTIALITY

Confidentiality implies that authorized individuals or systems can view sensitive or classified information, hence

restricting the access to unauthorized personnels. The main goal being to protect the information. The attacker may try to capture the data using his skills and the variety of tools available and acquire the privy information. A fundamental scheme to secure the data is by using encryption techniques, encryption basically is using an algorithm to encode the information into a format that could be read by only the person for whom it was meant.

Some of the common encryption standards include **AES**(Advanced Encryption Standard), 3 **DES** (Triple Data Encryption Standard), RSA (Rivest-Shamir-Adleman) and Twofish.

Another way to protect the data is to **implement a VPN tunnel**. VPN stands for Virtual Private Network and helps the data to move securely over the network. **A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.**

Other ways to ensure information confidentiality include **enforcing file permissions and access control list to restrict access to sensitive information.**

INTEGRITY

Integrity assures that the data or information system can be trusted. It ensures that information is in safe hands and is modified only by authorized personnels.

The purpose of this component is to restrict unauthorized modifications or to make sure that an option to undone changes is always available. Also, **integrity involves making sure that data is always consistent, accurate and trustworthy**.

Some methods used to ensure integrity are: **Typical system file permissions, user access control, version control. Backups and redundancy** are important to restore breaches of integrity. **Data encryption and hashing algorithms** are key processes in providing integrity.

We have two common types of hashing algorithms: **SHA (Secure Hash Algorithm) and MD5(Message Direct 5)**. Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, SHA-3.

There are two types of data integrity: physical and logical. **Physical integrity is basically the protection of data's accuracy as it is stored and retrieved.** The main threats to physical integrity are natural disasters, or a threat to the actual storage location of the server. **Logical integrity is basically protection of data from any unauthorized modifications.** This also protects information from errors by authorized personnels.

AVAILABILITY

This means that the **information should be readily available to its authorized users. This applies to systems and data.** To ensure availability, **the systems which store and process the information and the security systems function correctly.** Ensuring the information and systems are available also involves preventing attacks.

It also includes **maintenance of hardware**. Keeping the system updated with **system upgrades** and a well functioning operating system. Preventing occurrence of network bottlenecks, redundancy, failover and adaptive recovery management system.

To prevent the situation of data loss, a backup copy is advisable. Adding security elements like firewalls and proxy servers to safeguard the systems from DoS and DDoS attacks.

RISKS

Cybersecurity risk is the exposure to harm or result of the breaches or attacks of the information and systems or harm to the physical assets.

A **structured risk management process** involves:

1. **Identifying information and systems**, i.e which can be considered **as assets.** Also to **identify the potential threats, vulnerabilities and impacts.**
2. **Evaluating risks** and creating pointers on the damage that can be done.
3. Deciding **how to deal with the risks based on the impact,** i.e avoid, mitigate, share or accept them.
4. **Selecting or designing appropriate security controls and implementing them, wherever risk mitigation is required**.
5. **Monitoring the systems to make adjustments and improvements at security policies.**

Some of the risks of 2019 are, as published in Cybersecurity by Cisco:

1. Data Breach

A data breach is the release of private information to an unsecure or untrusted environment. The data might have been stolen, copied, transmitted or viewed.

2. Insecure Application User Interface (API)

Breaches through Application User Interface are caused by a lack of tight security, starting from the authentication to encryption. The solution to this is that you, as the client, should be keen on the security measures that your provider has put in place. Additionally,

the encryption and authentication process must be stringent. Some of the API security risks as per OWASP are Broken Object Level Authorization, Broken User Authentication, Excessive Data Exposure, Lack of Resources and Rate Limiting, Broken Function Level Authorization, Mass Assignment, Security Misconfiguration, Injection, Improper Assets Management, Insufficient Logging and Monitoring.

3. Cloud Abuse

The increase in usage of cloud for storage has made it susceptible to attacks. And the usage is as easy, provided you have a credit card, you have the key to signing up and using the cloud as soon as you are done. The simplicity, in turn, makes the cloud vulnerable to spam emails, criminals, and other malicious attacks. To mitigate the situation, it is advisable that cloud service providers develop authentication and registration processes. Additionally, they should have a way of monitoring all transactions. A thorough evaluation of network traffic is also crucial in eliminating cyber abuse.

4. Malware Attack

A malware attack refers to the activities of malicious software platforms that the owner of a system is not aware of. There are many causes of malware attacks.

5. Loss of Data

Important data may get lost due to many reasons. One may be through alteration, deletion, and use of an unreliable storage medium. Additionally, use SSL encryption to secure our data and evaluate the data protection plan of the provider.

6. Hacking

With the Internet of Things taking over, more weak points are created in the computer systems. There are many reasons that could open up vulnerabilities like weak systems, unprotected information, unauthorized access.

7. Single-factor passwords

Secure passwords with a minimum length and special characters with two- way authentication can be a key to protect the systems.

8. Insider Threat

Organizations will continue to face insider threats as a major form of cybersecurity breaches. **The users in organizations are a weak link.** This is not to mention the importance of monitoring the staff, training them on how to patch up weak points, and measuring their activity. Proper access granted to the right person is a key to protect from insider threat. Employers should recruit staff only after background checks and have a mechanism to monitor them after.

9. Internet of Things (IoT)

Most devices connect through the internet of things. This creates a wider surface to base attacks upon. As much as the internet of things has become useful, there are many concerns surrounding it. **Its deployment has brought along security concerns. Studies have shown that the IoT possesses architectural flaws like inadequate security measures stemming from weak points.**

Proper ways of deploying security systems and awareness will go a long way in ensuring the threat is under control.

10. Shadow IT Systems

Shadow IT is software used within an organization, but not supported by the company's central IT system. What causes a breach in shadow IT is the fact that the risk of data loss does not receive much attention when it comes to data backups. More so, there is no control over who gets to access the data. Also, the backup and recovery processes have no one to monitor. Due to these inefficiencies, you become vulnerable to hackers. To mitigate this, spread awareness regarding the security threat that shadow IT brings. Additionally, be sure to purchase shadow IT resources from a reputable vendor.

DATA BREACH

A data breach is a confirmed incident in which privy or otherwise protected data has been accessed, modified or disclosed in an unauthorized manner.

Common data breach **exposures include personal information, such as credit card numbers, Social Security numbers** and healthcare histories, as well as corporate information, such as customer lists, manufacturing processes and software source code.

If anyone who is not specifically authorized to do so views such data, the organization charged with protecting that information is said to have suffered a data breach.

If a data breach results in identity theft and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil litigation.

Data breaches can be brought about by weak passwords, missing software patches that are exploited or lost or stolen devices like laptop computers and mobile devices. Users **connecting to rogue wireless networks that capture login credentials** or other sensitive information in transit can also lead to unauthorized exposures.

Social engineering, especially attacks carried out via email phishing can lead to users providing their login credentials directly to attackers or through subsequent malware infections. Criminals can then use the credentials they obtained to gain entry to sensitive systems and records -- access which often goes undetected for months, if not indefinitely.

While hackers and cybercriminals often cause data breaches, **there are also incidents where enterprises or government agencies inadvertently expose sensitive or confidential data on the internet. These incidents are typically known as accidental data**

breaches, and they usually involve the organization's misconfiguration of cloud services or failing to implement the proper access controls, such as password requirements for public-facing web services or applications.

Sometimes hackers use their skills for personal motives.

Regulations regarding data breach

A number of industry guidelines and government compliance regulations mandate strict control of sensitive, often personal, data to avoid data breaches.

Within a corporate environment, for example, **the Payment Card Industry Data Security Standard (PCI DSS)** dictates who may handle and use sensitive PII, such as credit card numbers, in conjunction with names and addresses. **It is a widely accepted set of policies and procedures intended to help the security of credit, debit, and cash card transactions and protect cardholders against misuse of personal information.**

Within a healthcare environment, **the Health Insurance Portability and Accountability Act (HIPAA) regulates who may see and use PHI, such as a patient's name, date of birth, Social Security number and healthcare treatments.**

There are also specific requirements for the reporting of data breaches via HIPAA -- and its Health Information Technology for Economic and Clinical Health (HITECH) Act and Omnibus Rule -- as well as the various state breach notification laws.

How to prevent data breaches

There is no guarantee of a security product or control that can prevent data breaches. **The most reasonable means for preventing data breaches involve common sense security practices. This includes well-known security basics, such as conducting ongoing vulnerability and penetration testing, using proven malware protection, using strong passwords/passphrases and consistently applying the necessary software patches on all systems.** The above methods are the basic step to protect any system. The most important thing is to go through the privacy policy wherever personal information is required.

To protect the systems and environment, keeping the data protected by encrypting it and making sure that communications are done over a protected channel.

Additional measures for preventing breaches, as well as minimizing their impact, include **well-written security policies for employees and ongoing security awareness training to promote those policies and educate employees.**

Such policies may include concepts such as the **principle of least privilege (POLP), which gives employees the bare minimum of permissions and administrative rights to perform their duties.** In addition, organizations should have an **incident response plan (IRP) that can be implemented in the event of an intrusion or breach; an IRP typically includes a formal process for identifying, containing and quantifying a security incident.**

THREATS

A cyber threat is an act or possible act that intends to steal data (personal or otherwise), harm data or cause some sort of digital harm.

Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

The threat is a possible danger that might exploit a vulnerability. A vulnerability can be defined as a flaw or weakness in a system's design, implementation or operation, and management that could be exploited to violate the system's security policy.

ATTACKS

Corresponding to the various types of vulnerabilities to a system resource are threats that are capable of exploiting those vulnerabilities. **A threat represents potential security harm to an asset (An asset is a system resource that is, data contained in an information system; or a service provided by a system). An attack is a threat that is carried out (threat action)and, if successful, leads to an undesirable violation of security, or a threat consequence.**

An attack can be defined as an assault on system security that derives from an intelligent threat that is a deliberate attempt to violate the security policy of a system. The attacker who executes the attack is called the threat agent.

Attacks can be of two types, Active and Passive.

An active attack is an attempt to alter system resources or affect their operation. The active attack involves modification of the data stream or the creation of false statements. Some examples of active attacks are masquerade, modification of messages, repudiation, replay, denial of service, etc.

A Passive attack is an attempt to learn or make use of information from the system but does not affect the system resources. Passive attacks are in the nature of eavesdropping on or monitoring of transmission. The objective of the threat agent is to obtain information that is being transmitted. Some examples of passive attacks are the release of message content, traffic analysis, etc.

Attacks can also be classified on the basis of the origin of the attack, that is, inside and outside attack.

An Inside attack is initiated by an entity inside of the security perimeter (an insider). The attacker has authorized access to

the system resources but uses them is a way not approved by those who granted the authorization.

An Outside attack is initiated by an entity outside the perimeter, by an unauthorized or illegitimate user of the system. The potential outside attackers could be amateur pranksters, organized criminals, international terrorists, and hostile organizations.

Some of the threat actions and its consequences:

- Threat consequence- **Unauthorized Disclosure**

  A circumstance or event whereby an entity gains unauthorized access to data and systems.

  Threat action:

  1. **Exposure:**

     Sensitive data or privy information is directly released to an unauthorized entity.

  2. **Interception**:

     An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.

  3. **Interference**:

     A threat action whereby an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of characteristics.

  4. **Intrusion**:
     An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

- Threat consequence **-Deception**

  A circumstance or event that may result in an unauthorized entity receiving false data and assuming it to be true.

  Threat action:

  1. **Masquerade**:

     An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.

  2. **Falsification**:

     False data deceive an authorized entity.

  3. **Repudiation**:

     An entity deceives another by denying responsibility for an act that caused harm.

- Threat consequence- **Disruption**

  A circumstance or event that interrupts or prevents the correct operation of system services and functions.

  Threat action:

  1. **Incapacitation**:

     Prevents or interrupts system operation by disabling a system component.

  2. **Corruption**:

     Undesirably alters system operation by adversely modifying system functions or data.

3. **Obstruction:**

   A threat action that interrupts delivery of system services by hindering system operation.

- Threat consequence- **Usurpation**

  A circumstance or event that results in control of system services or functions by an unauthorized entity.

  Threat action:

  1. **Misappropriation**:

     An entity assumes unauthorized logical or physical control of a system resource.

  2. **Misuse**:

     It causes a system component to perform a function or service that is detrimental to system security.

EXPLOITS

An exploit is a successful attack that takes advantage of the vulnerability the system has to offer to the threat agents.

An exploit takes advantage of a weakness in an operating system, application or any other software code, including application plug-ins or software libraries. **The owners of the code typically issue a fix, or patch, in response.** Users of the system or application are responsible for obtaining the patch, which can usually be downloaded from the software developer on the web, or it may be downloaded automatically by the operating system or application that needs it. Failure to install a patch for a given problem exposes the user to a computer exploit and the possibility of a security breach. Users should be responsible to update the softwares with the patches released.

Some of the most common web-based security vulnerabilities are SQL injection attacks, cross-site scripting, and cross-site request forgery as well as abuses such as broken authentication code or security misconfigurations.

Exploits can be classified on the basis of how the exploit works and what type of attack it is capable of accomplishing. They can be categorized on the basis of the result of the attack and the type of vulnerability it attacks.

Exploits are generally launched by malicious websites and are often composed of two main components: the exploit code and the shellcode. The exploit code is the software that attempts to exploit a known vulnerability. The shellcode is the payload of the exploit. The software is designed to run once the target system has been breached. The shellcode gets its name from the fact that some of these payloads open a command

shell that can be used to run commands against the target system; however, not all shellcodes actually open a command shell.

INFORMATION GATHERING

Information gathering is one of the crucial steps for carrying out an attack. It is getting to know the system which offers a particular vulnerability that is to be exploited. This is first and foremost step to be take.Some of the techniques are:

SOCIAL ENGINEERING

Social Engineering is a technique employed by an attacker, who persuades an unaware user to give him access to confidential data, systems and networks. This technique completely relies on the interaction between threat actors and users. The threat actors conceal their identity and pose themselves as a trusted individual or information source.

This technique focuses on exploiting a user's weaknesses rather than to find a network or software vulnerability. It is the first step in infiltrating a system.

How does social engineering work?

The first and most important step is for the attacker to perform research and reconnaissance on the target. Their focus is on identifying behaviors and patterns in the information collected and exploiting the weakness uncovered during the reconnaissance phase. A lot of systems have loopholes, and reconnaissance basically is studying the system carefully to discover those loopholes that might have been left out while creating those systems.

The attack is designed based on the basis of the information collected during the recon phase. If the attack is successful the attacker gets access to

sensitive data like credit card number, social security number, address, mobile number, etc

Some of the common social engineering attacks are:

1. **Phishing**:

One of the leading forms of social engineering attacks that are delivered to the user through various interactions in the form of emails, chats, and websites that are designed to pose as a secure and real system and organization. These are basically to trick the user and manipulate them to share their confidential data with the attacker enabling him to install malware or spyware in the user's system.

2. **Baiting**:

The attacker leaves a malware-infected physical device, such as a USB flash drive, in a place that is sure to be found. The user finds the device and loads it in his computer and unintentionally installs the malware.

3. **Spear phishing:**

Spear phishing is similar to phishing but tailored for a specific individual or organization.

4. **Vishing**:

It is gathering personal and financial information from the target over phone calls. Vishing is basically voice phishing.

5. **Pretexting**:

Pretexting is when one person lies to another to gain access to privileged data. An attacker pretends to need personal or financial data in order to confirm the identity of the recipient.

6. Scareware:

Scareware involves tricking the victim into thinking that his computer is infected with some malware or has downloaded illegal content. The attacker then offers the victim a solution that will fix the current problem instead he is tricking the user to download and install the attacker's malware.

7. Water-holing:

A watering-hole attack is when the attacker attempts to compromise a specific group of people by infecting websites they are known to visit and trust, in order to gain access to the network.

8. Diversion theft:

In this type of attack, a diversion is created like tricking a delivery or courier company into going to wrong locations, thus intercepting the transaction.

9. Quid pro quo:

A quid pro quo attack is one in which the social engineer poses to be from a secure organization and contacts a group of people having a common profile as in working within the same organization and offering a solution to a problem and hence gaining access to system resources or passwords while pretending to help.

10. Honey trap:

An attacker poses to be an attractive person through fake social media profiles to interact with a person online, fake an online relationship and gather sensitive information through that relationship.

11. Tailgating:

This is sometimes also referred to as piggybacking. It is when an unauthorized person follows an authorized person to a secure facility such as a corporate area or system.

12. Rogue:

Rogue security software is a type of malware that tricks the targets into paying for the fake removal of malware

13. Eavesdropping:

The attacker tries to record personal conversations of the target victim with someone that's being held over a communication medium.

14. Shoulder Surfing:

In this technique, the attacker tries to catch the personal information like email id, password, etc; of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.

FOOTPRINTING

Footprinting means gathering information about a target system that can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. This is also a very important step for an ethical hacker; he can find possible attacks, vulnerabilities, and patch that.

During this phase, a hacker can collect the following information:

- ❏ Operating System of the target machine
- ❏ IP Addresses
- ❏ Firewall
- ❏ Network Map
- ❏ Security configurations of the target machine
- ❏ E-mail id, passwords, phone numbers
- ❏ URL's
- ❏ VPN

There are two types of footprinting:

1. **Active Footprinting:**

   Active footprinting means to perform footprinting by getting in direct touch with the target machine.

2. **Passive Footprinting:**

   Passive footprinting means collecting information on a system located at a remote distance from the attacker.

Some techniques, tools, commands used for footprinting are:

1. **Ping command:**

   ping <target IP address>/<target name>

   PING (Packet Internet Groper) command is the best way to test connectivity between two nodes., whether it is Local Area Network(LAN) or Wide Area Network(WAN). Ping uses ICMP (Internet Control Message Protocol) to communicate with other devices. You can ping the hostname of the IP address.

2. **WHOIS Lookup:**

   You can search for any IP address or domain name. You can simply enter the domain name whose information you'd like to view into the search field on the WHOIS main page. You can retrieve key information about a domain in this way including availability, ownership, creation, and expiration details.

   By using the WHOIS lookup, you can get phone numbers, email addresses, servers of your target websites, etc. Basically this serves a way for website footprinting.

3. **Using Neo Trace:**

   NeoTrace is a powerful tool for getting path information. The graphical display displays the route between you and the remote site, including all intermediate nodes and their information. NeoTrace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.

4. **An Organization's Website:**

It's the best place to begin for an attacker. If an attacker wants to look for open-source information, which is information freely provided to clients, customers, or the general public then simply the best option is: "ORGANIZATION's WEBSITE".

5. **Archieve.org:**

Archived version refers to the older version of the website which existed in a time before and many features of the website have been changed. archieve.org is a website that collects snapshots of all the websites at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.

Other notable methods of finding information are Social media sites, search engines like Google which offer basic search techniques combined with advanced operators can do great damage ex- "inurl:", "allinurl:", "filetype:" etc, Social engineering, etc.

SCANNING

Scanning refers to techniques and procedures used to identify hosts, ports, and various other services within a network.

Network scanning is one of the crucial components of intelligence gathering and information retrieving mechanism, to create an overview of the target organization.

Vulnerability scanning is performed by penetration testers to detect the possibility of network security attacks. This helps in the identification of missing patches, unnecessary services, weak authentication, or weak encryption algorithm.

Tools that can are used to scan networks and ports are:

1. **Nmap**: to extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions.
2. **Angry IP Scanner**: scans for systems available in a given input range.
3. **Hping2/Hping3:** are command-line packet crafting and network scanning tools used for TCP/IP protocols.
4. **Superscan:** is another powerful tool developed by Mcafee, which is a TCP port scanner, also used for pinging.
5. **ZenMap:** is another very powerful Graphical user interface (GUI) tool to detect the type of OS, OS version, ping sweep, port scanning, etc.
6. **Net Scan Tool Suite Pack:** is a collection of different types of tools that can perform a port scan, flooding, web rippers, mass mailers, and This tool is a trial version, but paid versions are also available.

7. Wireshark and Omnipeak are two powerful and famous tools that listen to network traffic and act as a network analyzer.

8. Names of other famous tools for PCs are Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer, etc.

9. Tools and software that are used in mobiles as scanners include the names such as Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Panm IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc.

10. Banner Grabbing: This method is used for obtaining information regarding a targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack. This information may be used by intruders/hackers to portray the lists of applicable exploits.

TOOLS

NMAP

Nmap, Network mapper is a free and open-source network scanner created by Gordon Lyon. It discovers the hosts and services on a given computer network by sending packets and analyzing responses.

It not only helps to discover the hosts and services running on a network but also the operating system detection, port scanning and vulnerability detection.

Nmap can be used to test a firewall, auditing open ports, network mapping and maintenance, finding and exploiting vulnerabilities, subdomain search.

ZENMAP

Zenmap is the official Nmap Security Scanner GUI.

PORT SCANNER

A port scanner is an application designed to scan the host for open ports. It is used to verify security policies of the networks or to exploit vulnerabilities by identifying network resources running on a host machine.

A port scan is a process in which the client requests to connect with a range of port addresses on the host, to find an active port.Th emost common types of scans include TCP, SYN, UDP,ACK, Window, FIN, etc.

NETWORK SCANNER

Network scan gives the user or the admin the insight into the username and info about the groups and services about the systems in a network. It is different from Nmap, as Namp only gives information about the servers connected to a specific network.

CHAPTER 2
CRYPTOGRAPHY AND CRYPTANALYSIS

SUBTOPICS:

Introduction to Cryptography, Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls-Types of Firewalls, User Management, VPN Security, Security Protocols:- Security at Application Layer-PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.
Open Source/ Free/ Trial Tools: Implementation of Cryptographic techniques, OpenSSL, Hash Values Calculations

MD5, SHA1, SHA256, SHA 512, Steganography (Stools)

What is Cryptography?

Cryptography is a technique of securing information and communications through the use of codes so that only the authorized person can access it. It is to keep away third parties called adversaries. The prefix “crypt” means “hidden” and suffix “graphy“ means “writing”. Earlier they were confined only to encryption.

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Cryptography is based around designing computationally secure algorithms. These algorithms are difficult, but not impossible, to figure out. The biggest factor that makes an algorithm secure is the difficulty and the number of resources involved in figuring it out.

Some essential terms are:

Encryption:

Encryption is the basis for cryptography, it is the transformation of readable important information to the incomprehensible/intelligible form, which is called ciphertext.

Decryption:

Decryption is the complementary process to bring the ciphertext back to normal language or plain-text.

Cipher:

A cipher is a set of algorithms from which the encryption or decryption result.

Key:

It is the instructions for decoding the encrypted data.

Cryptosystem:

A cryptosystem is a set of possible cryptography elements that could match up to a key.

Cryptanalysis:

Cryptanalysis is the study of how to crack the encryption. That is method of obtaining the meaning of encrypted information without access to the key which is normally required to do so.

SYMMETRIC KEY CRYPTOGRAPHY

It is also known as symmetric encryption. **It is an encryption system where the sender and the receiver of message use a single common key to encrypt and decrypt messages. Symmetric key systems are faster and simpler but the problem is that the sender and receiver have to somehow exchange the key in a secure manner.** This was the only known kind of encryption publicly known until the mid 1970's. The most popular symmetric-key cryptography system is the Data Encryption System (DES).

Most symmetric-key ciphers are either block ciphers, where **the input and output text is the same size**(ex- 128-bit plaintext is encrypted into 128-bit ciphertext), or **stream ciphers, which create a**

long key that is combined with the plain-text that is to be encoded(ex-1 bit of plaintext is encrypted into 1-bit ciphertext at a time). It is sometimes referred to as **conventional encryption or single-key encryption.**

Symmetric encryption scheme has five ingredients

1. **Plaintext:**

   This is the original message or data that is fed into the algorithm as input.

2. **Encryption algorithm:**

   The encryption algorithm performs various substitutions and transformations on the plaintext.

3. **Secret key:**

   The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

4. **Ciphertext:**

   This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

5. **Decryption algorithm:**

   This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plain text.

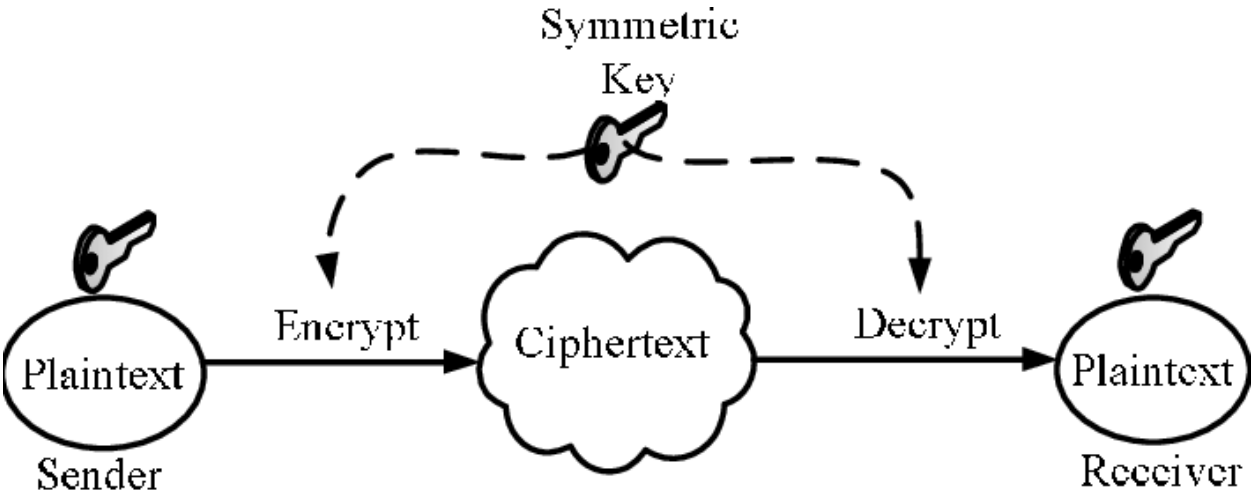


Image source-researchgate.net

The security of symmetric encryption systems is based on how difficult it is to randomly guess the corresponding key to brute force them. The longer the encryption key, the harder it becomes to crack it. **Keys that are 256-bits length are generally regarded as highly secure and theoretically resistant to quantum computer brute force attacks.**

There are two requirements for secure use of symmetric encryption:

1. **A stronger encryption algorithm, the algorithm should be such that an opponent who knows the algorithm and has access to one more ciphertexts would be unable to decipher the ciphertext or figure out the key.** This requirement is usually started in a stronger form: The opponent should be unable to decrypt the ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. **Sender and receiver must have obtained copies of the secret key in a secure way and must keep the key secure.** If someone can discover the key and knows the algorithm, all communication using this key is readable.

There are two general approaches to attacking a symmetric encryption scheme. The first attack is known as cryptanalysis. **Cryptanalytic attacks rely on the nature of algorithms and some knowledge of general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.** This type of attack **exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.** If the attack succeeds in deducing the key, all future and past messages encrypted with that key are compromised. There are two possible approaches. The cryptanalyst is in possession of ciphertext and wants to decrypt to plaintext. The second way being that the cryptanalyst in possession of ciphertext wants to know about the key that was used.

The second method, known as **the brute-force attack, is to try every possible key on a piece of ciphertext until an intelligible**

translation into plaintext is obtained. It is not an efficient way. If the key length is long enough, it isn't feasible. There is no way to defend against a key search attack as there isn't a way to keep an attacker from trying all the keys. Some examples of symmetric encryption algorithms include:

1. **AES (Advanced Encryption Standard)**
2. **DES (Data Encryption Standard)**
3. **IDEA (International Data Encryption Algorithm)**
4. **Blowfish**
5. **RC4 (Rivest Cipher 4)**
6. **RC5 (Rivest Cipher 5)**
7. **RC6(Rivest Cipher 6)**

In the above listed examples AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers while RC4 is a stream cipher.

DATA ENCRYPTION STANDARD

The most widely used encryption scheme is based on the Data Encryption Standard adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FISP PUB 46). The algorithm in itself is known as Data Encryption Algorithm (DEA). DES takes a plaintext block of 64 bits and a key of 56 bits, to produce a ciphertext block of 64 bits.

Concerns about the strengths of DES fall into two categories: concerns about the algorithm itself and concerns regarding the usage of a 56-bit key. The first concern raises over the ability of cryptanalysis in exploiting the characteristics of the DES algorithm. The second concern was about the key length. With a key length of 56 bits, there are 2^{56} keys possible.

DES was proved insecure in 1998 by a special purpose “DES cracker” machine made by Electronic Frontier Foundation. The EFF approach addressed the issue that to supplement the brute-force approach, some knowledge about the expected plaintext is needed and an automated way of distinguishing the plain-text from garble. Increasing the key length to 128-bit key is guaranteed to result in an algorithm that is unbreakable by brute-force.

The practically secure version of DES is the triple DES (3DES) which involves repeating the basic DES algorithm three times, using either two or three unique keys, for a key size of 112 or 168 bits. 3DES had two major attractions. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES. Second, the underlying encryption algorithm in 3DES is the same as in DES. After a longer period of scrutiny, it was found that no effective cryptanalytic attack based on the algorithm rather than brute force has been found.

The principal drawback of 3DES is that the algorithm is relatively sluggish in software. The original DES was designed for mid-70's hardware implementation and does not produce efficient software code. 3DES, which requires three times as many calculations as DES, is correspondingly slower. A secondary drawback is that both DES and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.

DES is a block cipher, an algorithm that takes a fixed-length string of plaintext bits and after a series of transformations a ciphertext is obtained. The block size is 64 bits and the key consists of 64 bits, 56 bits are to be used by algorithm and 8 bits are used as parity checker and are discarded afterwards.

ADVANCED ENCRYPTION STANDARD

As a replacement to 3DES, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have strength equal to or better than 3DES and significantly improved efficiency. In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.

In 2001, AES was issued as a federal information processing standard (FIPS 197). NIST had selected Rijndael as the proposed AES algorithm out of the 15 algorithms received for evaluation.

AES is a subset of the Rijndael block cipher developed by Vincent Rimjen and Joan Daemen. Rijndael is a family of ciphers with different key and block sizes.

Typically, symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block. Plaintext sources must be broken up into a series of fixed-length blocks for encryption by a symmetric block cipher. The simplest approach to multiple-block encryption is known as electronic codebook (ECB) mode.

For lengthy messages, the ECB mode may not be secure. A cryptanalyst may be able to exploit regularities in the plaintext to ease the task of decryption. To increase the security of symmetric encryption for large sequences of data, a number of alternative techniques have been developed, called modes of operation.

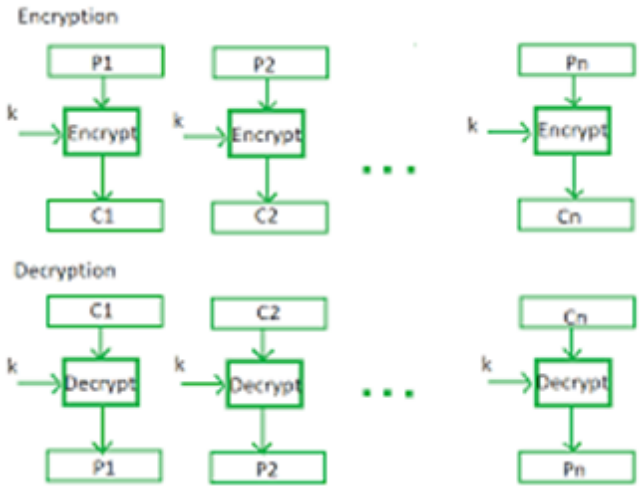


Image Source- geeksforgeeks

STREAM CIPHERS

It is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. A typical stream cipher encrypts 1 byte of plaintext at a time, although it can be made to work with 1 bit at a time or on units larger than a byte at a time. The encryption of each digit is dependent on the current state of the cipher, it is also known as a state cipher.

In this structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. A pseudorandom stream is one that is unpredictable without knowledge of input key and which has an apparently random character. The output of this generator, called a keystream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation.

A pseudorandom key is generated serially from a random seed value using digital shift registers. The seed value is used for decrypting the ciphertext stream.

With a properly designed pseudorandom number generator, a stream cipher can be as secure as a block cipher of comparable key length. The primary advantage of stream ciphers is that stream ciphers are almost always faster and use far less code than the block ciphers. The advantage of the block cipher is that you can reuse the keys. The stream ciphers are susceptible to problems if applied incorrectly, that is the initial seed (used as starting state) must never be used twice.

For applications that require encryption/ decryption of a stream of data, such as over a data communications channel or a browser/web link, a stream cipher may be a better alternative. For applications that deal with a block of data, such as file transfer, e-mail and database, block ciphers are appropriate. However, either one can be used in virtually any application.

ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography is also known as public-key cryptography. Public key algorithms are based on mathematical functions to produce one-way functions rather than on simple operations on bit patterns, such as are used in symmetric encryption algorithms. More importantly it's called asymmetric, as it consists of pairs of keys:public key, which are available to all and private key, which is known only to the user, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution and authentication.

A public-key encryption scheme has six ingredients:

1. **Plaintext:**

This is the readable data or message that is fed into the algorithm as input, i.e. information that is to be transmitted.

2. **Encryption algorithm:**

The encryption algorithm performs various transformations and substitutions on the plaintext.

3. **Public and private key:**

This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.

4. **Ciphertext:**

This is the unintelligible message produced as output. It depends on the plaintext and the key.

5. Decryption algorithm:

This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

As the name suggests, the public key of the pair is made public for others to use, while the private key is known only to its owner. A general-purpose public-key cryptographic algorithm relies on one key for encryption and a different but related key for decryption.

The essential steps are the following:

1. **Each user generates a pair of keys to be used for the encryption and decryption of the messages.**
2. **Each user places one of the two keys in a publicly accessible resource. This is the public key. The other key is kept private.** Each user maintains a collection of public keys obtained from others.
3. **If the sender wishes to send a private message to the receiver, then he/she will encrypt the message using the public key of the receiver.**
4. **When the receiver gets the message, he/she decrypts it using the private key.** No other user will be able to decrypt the message except for the intended person, as only that person would know the private key to decrypt the message.

Another mode of operation of public-key cryptography would be that a user encrypts data using his or her own private key. Anyone who knows the corresponding public key will then be able to decrypt the message.

The earlier approach is directed towards providing confidentiality: Only the intended recipient or the presumed owner should be able to decrypt the ciphertext because only that person is in possession of the required private key. The **confidentiality** provided also depends on a

number of factors, including the security of the algorithm, whether the private key is kept secure and the security of any protocol of which encryption function is a part.

In the second approach mentioned, is directed towards providing authentication and/or data integrity. If a user is able to recover the plaintext from the ciphertext using the sender's public key, this indicates that only the sender could have encrypted the plaintext, thus providing authentication and assurity that information wasn't tampered. Hence, assuring **data integrity.**

MESSAGE AUTHENTICATION

Message Authentication also known as data origin authentication is a way to assure data integrity, that is the receiver can verify the source of the message and also be sure that data wasn't modified in transit. Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transactions). Protection against such attacks is known as message or data authentication.

Message or data authentication is a procedure that allows communicating parties to verify that received or stored messages are authentic. The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic. It can be achieved by message authentication codes (MACs) or digital signatures. The MAC or the digital authenticator pretty much works on a comparison based on the secret key shared between the sender and receiver. It is mostly based on the hash function but can be done by symmetric encryption.

To maintain the secrecy and avoid brute-force attacks, the key generated should be random. This is useful only where the communication is between two people exactly, with a third person present the authenticity of data is questionable.

MESSAGE AUTHENTICATION CODE

AUTHENTICATION USING SYMMETRIC ENCRYPTION

If we assume that only the sender and receiver share a key, then only the genuine sender would be able to encrypt the message successfully for the other participant, provided the receiver can recognize a valid message. Furthermore, if the message also includes a timestamp, the receiver is assured that the message has not been delayed beyond that normally expected for network transit.

In fact, symmetric encryption alone is not a suitable tool for data authentication. One of the examples is ECB mode of encryption, even if the attacker decrypts the blocks of ciphertext, reordering may alter the meaning of the overall data sequence. Thus, block reordering is a threat.

The sender uses a MAC algorithm that takes the information to be transmitted and secret key as input and produces a MAC value. A MAC function is known to compress a long input into an output of fixed length. The sender sends the message along with the MAC value.

The receiver, after getting the message, computes the MAC value in a similar way and compares it to the one received. If the receiver's MAC value checks with the sender's MAC value then the message is from the intended sender. To assure confidentiality the message should be sent in an encrypted or intelligible manner.

USING HASH FUNCTION

To define a hash function, it is a mathematical function that converts a numerical input value to a compressed one.This process is known as **hashing** the data. **The output always is of a fixed length.** Using a hash function differs from using symmetric encryption as while compressing the message a key is used incase of symmetric key encryption.

The compressed value returned by the hash function is known as **message digest or hash value**. Hash function not only protects the input message but also from substitution of another input message in case the attacker has the original message's hash.

The hashing algorithm involves breaking up the message in data blocks typically of size 128-512 bits. Hashing algorithm is similar to block cipher. It involves rounds of hash function. The process is repeated until the entire message has been hashed. Each round takes a new block and output of the current block as input. The hash of the first block is an input to hashing the second block, whose hashing will further affect the third. This is known as the **avalanche effect of hashing**.

DIGITAL SIGNATURE

Public-key encryption can be used for authentication. The sender uses a secure hash function like SHA-512 or MD5, to generate a hash value for the message and then encrypts the hash code with his private key, creating a digital signature.

The sender sends the message with the signature attached. The receiver gets the message along with the signature. The receiver:

1. Calculates a hash value for the message.
2. Decrypts the signature using the sender's public key.
3. Compares the calculated hash value to the decrypted hash value.

If the two hash values match, the receiver can be assured that the message is signed by the sender.

No one else has the sender’s private key and therefore no one could have created the ciphertext that could be decrypted by the sender’s public key. It is impossible to alter the message without access to the sender's private key, so the message is authenticated both in terms of source and in terms of data integrity.

It is important to emphasize that the digital signature does not provide confidentiality. That is, the message being sent is safe from alteration but not safe from eavesdropping. This is obvious in the case of a signature based on a portion of the message, because the rest of the message is transmitted in the clear. Even in the case of complete encryption, there is no protection of confidentiality because any observer can decrypt the message by using the sender’s public key.

APPLICATIONS OF CRYPTOGRAPHY

1. Earlier as seen, Message authentication code is used to protect the information in transit and also helps us in confirming that the data isn't modified and it is in its true form.

2. Digital signatures help in confirming the indenting of the sender to the receiver.

3. Cryptography allows storing the encrypted data permitting users to be assured that their message is beyond the reach of an attacker.

FIREWALLS

Firewall can be considered as an essential way to block network-based threats from protecting a local system or all the systems in a network. It monitors the incoming and outgoing network traffic and decides the permeability of the packets based on the security rules laid for it to follow.

The main objective is to protect the system from any malicious objects from external sources. It acts as a barrier between the internal network and the websites that the system is trying to access.

Firewalls watch the traffic at the entry point for information exchange, that is the computer ports.

To begin with the firewalls are classified basically to two types- software and hardware. A software firewall is a program installed to regulate and block the traffic through ports. A hardware firewall is placed between the network and gateway.

TYPES OF FIREWALLS

1. **Packet Filtering:**

This is the most basic type of firewall, they check all the data packets coming through the router, information about the source and destination IP addresses, packet type, port number. They are simple and inspect the packet received without causing harm to the contents of the packets.

2. **Stateful Inspection Filtering**:

This type of firewall alongwith packet-filtering firewall uses TCP handshake mechanism to deduce the reliability of the application. These firewalls may cause a delay in transmission of the data packets.

3. **Application Layer Firewalls:**

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic. These firewalls set up a proxy which not only verifies the TCP handshake and implements the packet filtering but also performs inspection on the contents of the data packet. After a heads up, the content is forwarded from the proxy to the actual destination.

4. **Circuit Level Gateway:**

These work on the Session layer to confirm that TCP handshakes between packets are legitimate. It does not examine the packet contents though. If a packet contains malware, it would pass through this barrier because of the right TCP handshake.

5. **Stateful Multilayer Inspection:**

These are a combination of packet filtering, circuit level gateways, and application layer firewalls.

USER MANAGEMENT

User management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks and more. User management is a core part to any service and is basic security essential for any organization. User management enables admins to control user access and on-board and off-board users to and from IT resources. Subsequently a service will then authenticate, authorize, and audit user access to the IT resources based on what the admin has dictated.

User management is a key procedure to protect the sensitive information held by a company from unauthorized access. If the Access lists are maintained timely by the admins the data can be protected from unwanted users.

VIRTUAL PRIVATE NETWORKS

In essence, a VPN uses encryption and authentication, extends a private network across a public network to provide a secure connection through an otherwise insecure network, thus providing functionality, security and management of the private network. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.

The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec. The private network connection can be established using an encrypted layered tunneling protocol, and users may have to authenticate in order to gain access to the VPN.

VPN protocols ensure an appropriate level of security to connected systems when the underlying network infrastructure alone cannot provide it. There are several different protocols used to secure and encrypt users and corporate data. They include:

1. IP security (IPSec)
2. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
3. Point-to-Point Tunneling Protocol (PPTP)
4. Layer 2 Tunneling Protocol (L2TP)
5. Open VPN

TYPES OF VPN

1. **REMOTE ACCESS VPN:**

   Remote access VPN clients connect to a VPN gateway server on the organization's network. The gateway requires the device to authenticate its identity before granting access to internal network resources such as file servers, printers and intranets. This type of VPN usually relies on either IP Security (IPSec) or Secure Sockets Layer (SSL) to secure the connection.

2. **SITE-TO-SITE VPN**

   It uses a gateway device to connect an entire network in one location to a network in another location. End nodes devices in the remote location do not need VPN clients because the gateway handles the connection. Most site-to-site VPNs connecting over the internet use IPSec.

3. **MOBILE VPN**

   In a mobile VPN, a VPN server still sits at the edge of the company network, enabling secure tunneled access by authenticated, authorized VPN clients. Mobile VPN tunnels are not tied to physical IP addresses, however. Instead, each tunnel is bound to a logical IP address. That logical IP address sticks to the mobile device no matter where it may roam. An effective mobile VPN provides continuous service to users and can seamlessly switch across access technologies and multiple public and private networks.

4. HARDWARE VPN

Hardware VPNs offer a number of advantages over the software-based VPN. In addition to enhanced security, hardware VPNs can provide load balancing to handle large client loads. Administration is managed through a web browser interface. A hardware VPN is more expensive than a software VPN.

SECURITY PROTOCOLS

A sequence of operations that ensure protection of data. When a security protocol is used with a communication protocol, it provides a secure path for delivery of data between two users.

SECURITY AT APPLICATION LAYER

Application layer security refers to ways of protecting web applications at the application layer from malicious attacks.

Since the application layer is closest to the end user, it provides hackers with the largest threat surface. Poor application layer security can lead to performance and stability issues, data theft, and in some cases the network being taken down.

Some of the examples of attacks at the application layer include distributed denial-of-surface attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, etc. Some of the ways to battle these malicious attacks are web application firewalls, secure web gateway services etc.

PGP (Pretty Good Privacy)

PGP stands for Pretty Good Privacy which is invented by Phil Zimmermann. PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication and non-repudiation in sending of an email. PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. PGP is an open source and freely available software package for email security. It provides confidentiality through use of symmetric block encryption.

Steps taken by PGP to create secure email at the sender site:

1. The e-mail message is hashed by using a hashing function to create a digest.
2. The digest is then encrypted to form a signed digest by using the sender's private key, and then the signed digest is added to the original email message.
3. The original message and signed digest are encrypted by using a one-time secret key created by the sender.
4. The secret key is encrypted by using a receiver's public key.
5. Both the encrypted secret key and the encrypted combination of message and digest are sent together.

Steps taken by PGP at the receiver's end:

1. The receiver receives the combination of encrypted secret key and message digest is received.

2. The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
3. The secret key is then used to decrypt the combination of message and digest.
4. The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
5. Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

MIME/S

Multipurpose Internet Mail Extension (MIME) is a standard which was proposed by Bell Communications in 1991 in order to expand limited capabilities of email. It is a supplementary protocol which allows non-ASCII data to be sent through SMTP (Simple Mail Transfer Protocol).

The drawbacks of SMTP were the reason for the need of MIME. Some of them are:

Simplicity of SMTP structure. It however can only send messages in 7-bit ASCII format. It cannot be used for languages that do not support 7-bit ASCII format such as French, German, Russian, Chinese,etc, so it cannot be transmitted using SMTP. SMTP cannot be used to send binary files or video or audio data.

Features of MIME –

1. It is able to send multiple attachments with a single message.
2. Unlimited message length.
3. Binary attachments (executables, images, audio, or video files) which may be divided if needed.
4. MIME provided support for varying content types and multi-part messages.

Working of MIME –

1. Suppose a user wants to send an email through a user agent and it is in a non-ASCII format so there is a MIME protocol which converts it into 7-bit NVT ASCII format.

2. Message is transferred through the e-mail system to the other side in 7-bit format now MIME protocol again converts it back into non-ASCII code and now the user agent of the receiver side reads it and then information is finally read by the receiver.
3. MIME header is basically inserted at the beginning of any email transfer.

SECURITY AT TRANSPORT LAYER

SECURE SOCKETS LAYER (SSL)

Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network. It was developed by Netscape, SSL technology creates a secure link between a web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for communication.

In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network. When using SSL for secure internet transactions, a web server needs an SSL certificate to establish a secure SSL connection. SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.

SSL follows an asymmetric cryptographic mechanism, in which a web browser creates a public key and a private (secret) key. The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only.

The objectives of SSL are:

- Data integrity: Data is protected from tampering.
- Data privacy:Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
- Client-Server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.

TRANSPORT LAYER SECURITY (TLS)

Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the internet. It enables privacy, integrity and protection for the data that is transmitted between different nodes on the internet. TLS is a successor to the secure socket layer (SSL) protocol.

TLS enables secure web browsing, application access, data transfer and most internet-based communication. It prevents the transmitted/transported data from being eavesdropped or tampered. TLS is used to secure web browsers, web servers, VPNs, database servers and more. TLS protocol consists of two different layers of sub-protocols:

1. **TLS Handshake Protocol:**

   Enables the client and the server to authenticate each other and select an encryption algorithm prior to sending the data.

2. **TLS Record Protocol:**

   It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

SECURITY AT NETWORK LAYER

IPSEC

The IP Security (IPSec) is a standard protocol between two communication points across the IP network that provides data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP security:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPSec tunneling in which all data being sent between two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security:

1. **Encapsulating Security Payload (ESP):**

   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

2. **Authentication Header (AH):**

   It also provides data integrity, authentication, and anti replay and it does not provide encryption. The anti replay protection protects against unauthorized transmission of packets. It does not protect data's confidentiality.

3. Internet Key Exchange (IKE):

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between two devices. The Security Association establishes shared security attributes between two network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Secure Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPSec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP Sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are unauthorized are discarded and not given to the receiver.

Working of IPSec:

1. The host checks if the packet should be transmitted using IPSec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host whether they are encrypted properly or not.
2. Then the IKE Phase 1 starts in which the two hosts (using IPSec) authenticate themselves to each other to start a secure channel. The Main mode provides greater security and the Aggressive mode enables the host to establish an IPSec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with these algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec's SAs.
6. When the communication between the hosts is completed or the session times out then the IPSec tunnel is terminated by discarding the keys by both the hosts.

TOOLS

OPEN SSL

OpenSSL is a toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is a software library for applications that secure communications over computer networks to secure it from eavesdropping or to verify the sender.

CHAPTER 3
INFRASTRUCTURE AND NETWORK SECURITY

SUBTOPICS:

Introduction to System Security, Server Security, OS Security, Physical Security. Introduction to Networks, Network packet Sniffing, Network Design Simulation. DOS/ DDOS attacks. Asset Management and Audits, Vulnerabilities and Attacks. Intrusion detection and Prevention Techniques, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.

Open Source/ Free/ Trial Tools: DOS Attacks, DDOS attacks, Wireshark, Cain & abel, iptables/ Windows Firewall, snort, suricata, fail2ban

SYSTEM SECURITY

A system is said to be secure if its resources are used and accessed by authorized personnels under all the circumstances and without any break-ins, but no system can guarantee absolute security from the various malicious threats and unauthorized access.

Security of a system can be threatened via two violations:

1. **Threat**:

   A program which has the potential to cause serious damage to the system.

2. **Attack**:

   An attempt to break security and exploit a vulnerability in the system and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental. Malicious threats are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches. Accidental threats are due to an undetected flaw during the designing of the system. Example:Denial of service DDoS attack.

Security can be compromised via breach of confidentiality, integrity, availability, theft and denial of service.

The sole purpose of system security was to maintain integrity, secrecy, and availability of all resources to the permitted users. Threats can be classified into two categories :

1. **Program Threats:** A program written to change the normal execution of a process(A process is a running program). Example- Virus, Trojan horse, trap door, logic bomb, etc.
2. **System Threats:** These threats involve the abuse of system services. They are created to interrupt normal execution of operating system, system services and user files. They are also used as a medium to launch program threats. Example- Worm, denial of service attack, etc.

SERVER SECURITY

A server can be explained as a computer program, providing a service to another computer program and it's usually referred to as the client. In a data center, the server program is run on a physical computer which is called the server. Server basically interconnects machines in a network. The different types of servers are FTP servers, online game servers and web servers.

The key functionality of a computer server is to store, retrieve and send data and files to other computers in a network upon request. On a larger scale, the internet, the worldwide computer network relies on a large number of servers located around the world for easy exchange of data.

As the server interconnects computers, they are the hub of a lot of valuables that can be accessed. Protection of this accessible information asset from a web server is known as server security. A security rupture can harmfully affect the goodwill as well as the monetary status of an organization.

Some of the mistakes that can cause the server to be less secure are passwords, open network ports, old software version, poor physical security, insufficient security of CGIs, old and unnecessary accounts, procrastination etc.

OPERATING SYSTEM SECURITY

Operating system security is the process of ensuring OS integrity, confidentiality and availability. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets worth of being stolen, edited or deleted if the OS security is compromised.

OS security may be approached in many ways, including adherence to the following:

1. Performing regular OS patch updates.
2. Installing updated antivirus engines and software.
3. Scrutinizing all incoming and outgoing network traffic through a firewall.
4. Creating secure accounts with required privileges only (i.e., user management).

PHYSICAL SECURITY

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, institution. This includes protection from natural calamities, burglary, theft, vandalism and terrorism.

Physical security is as important as other technical threats such as hacking, malware etc. The breaches of physical security can be carried out with brute force and little or no technical knowledge on the part of an attacker.

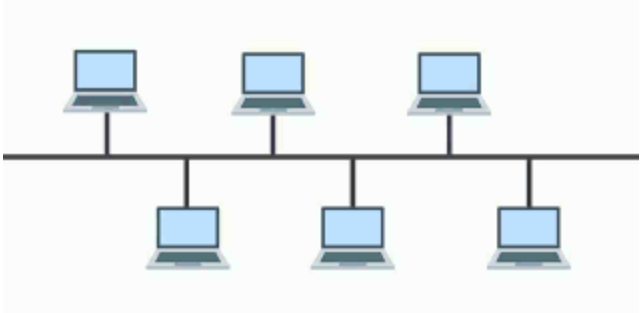
Physical security has three important components: access control, surveillance and testing. Obstacles should be placed in the way of potential attackers and physical sites should be hardened against accidents, attacks or environmental disasters.

INTRODUCTION TO NETWORKS

A network is a collection of computers, servers, mainframes, network devices, peripherals or other devices connected to one another to allow the sharing of data.

The term network topology describes the relationship of connected devices in the terms of geometric graphs. Devices are represented as vertices, and their connections are represented as edges of the graph. It describes how many connections each device has, in what order, and in what sort of hierarchy.

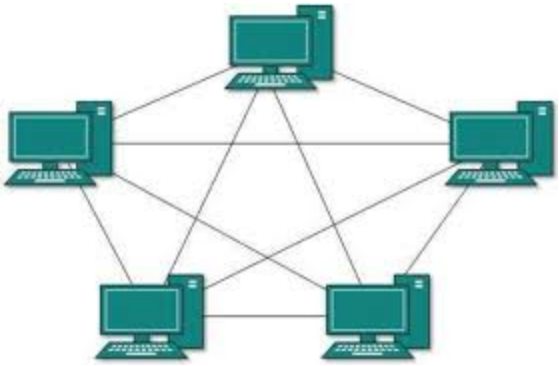
Typical network configurations include the bus topology, mesh topology, ring topology, star topology, tree topology and hybrid topology. Another classification of networks based on size is LAN (Local Area Network), PAN (Personal Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).



BUS TOPOLOGY

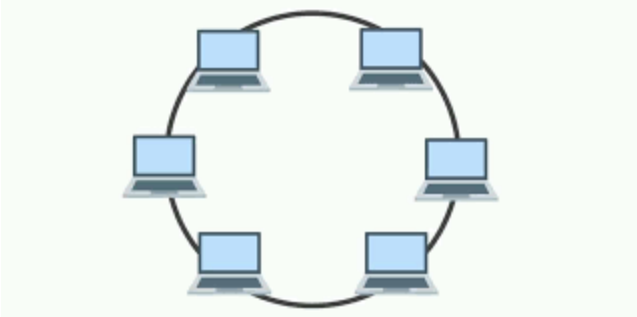
While using bus topology, each node is connected by interface to a central line. All data communicated between the nodes is transmitted over this

common transmission medium and is able to be received by all nodes in a network simultaneously.



MESH TOPOLOGY

In mesh topology, each node is connected to every other node in the network through a separate dedicated line for each connection. Each line is connected to two devices creating a unique connection.

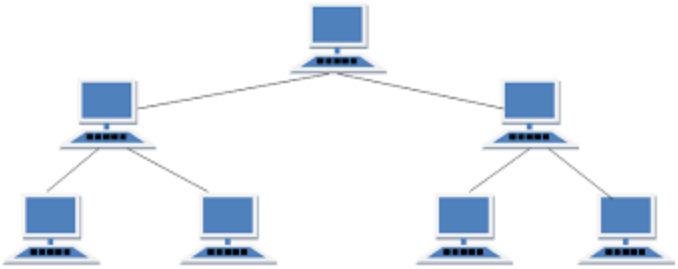


RING TOPOLOGY

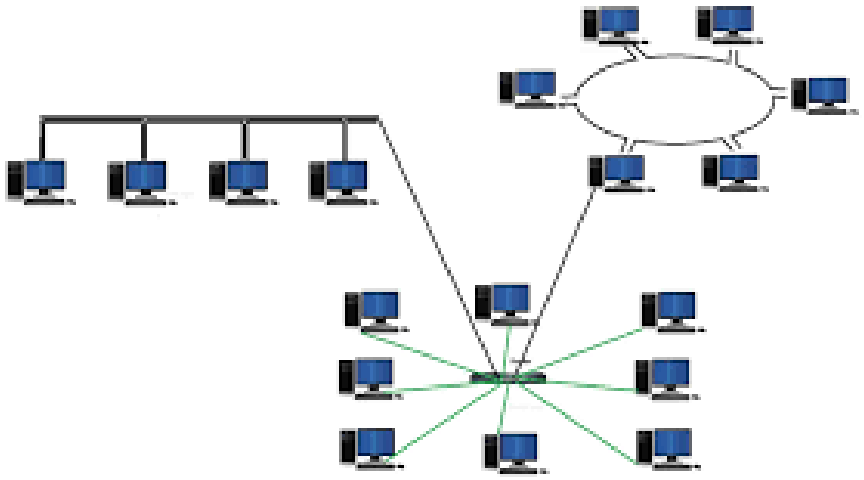
In ring topology, nodes are connected to a single line. Each node is connected to two others on either side of it. The structure forms a ring.

STAR TOPOLOGY

In star topology, each device in the network is connected to a central device. Star topology doesn't allow direct communication between devices.



TREE TOPOLOGY



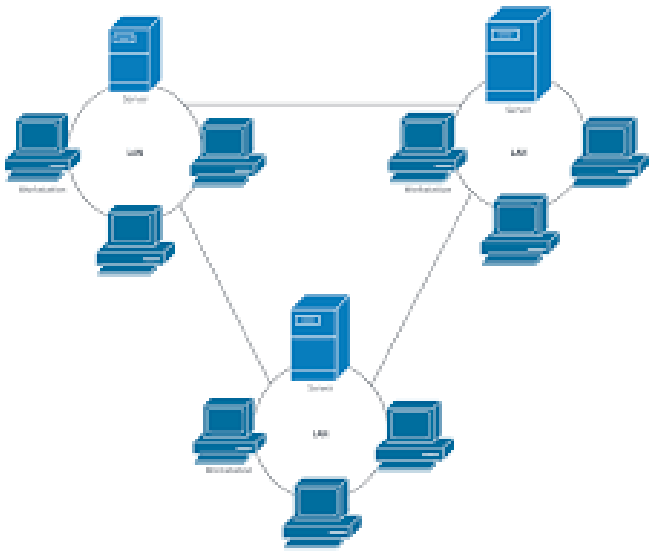
HYBRID TOPOLOGY

A combination of two or more topologies is called a hybrid topology.

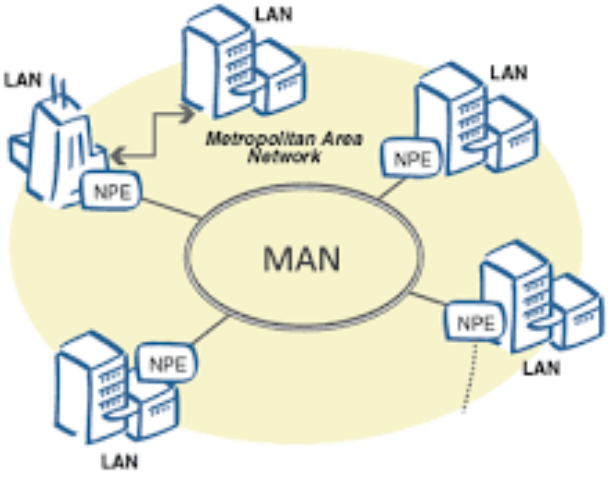
CLASSIFICATION BASED ON SIZE

LOCAL AREA NETWORK (LAN)

PERSONAL AREA NETWORK (PAN)



WIDE AREA NETWORK (WAN)



METROPOLITAN AREA NETWORK (MAN)

NETWORK PACKET SNIFFING

When any data has to be transmitted over the computer network, it is broken down into smaller units called data packets and reassembled at the receiver's node in original format. It is the smallest unit of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packets across the computer network is called packet sniffing.

It is mostly used by crackers and hackers to collect information illegally about networks. It is also used by ISPs, advertisers and governments. ISPs use packet sniffing to track all your activities such as who is the receiver of your email, what is the content of that email, what you download, sites you visit, what you looked on that website, downloads from a site, streaming events, etc.

Government agencies use packet sniffing to ensure security of data over the network, track an organization’s encrypted data, etc.

Advertising agencies or internet advertising agencies are paid according to the number of ads shown by them and number of clicks on their ads also called PPC (pay per click). To achieve this target, these agencies use packet sniffing to inject advertisements into the flowing packets. Most of the time these ads contain malware.

Packet sniffing is done by using tools called packet sniffer. It can be either filtered or unfiltered. Filtered is used when only specific data packets have to be captured and unfiltered is used when all the packets have to be captured. WireShark, SmartSniff are examples of packet sniffing tools.

NETWORK DESIGN SIMULATION

A network discovery software provides a way for a network administrator to map the hardware and software on his or her network. Network design and simulation software can let you test the network under different traffic loads and a variety of failure conditions.

Some of the different network simulators are:

- Ns2 (Network Simulator 2)

  It is a simulator that provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks. It uses C++ and OTcl languages.

- Ns3 (Network Simulator 3)

  Ns3 uses C++ and python languages for simulating the script. C++ is used for implementation of simulation and core models. NS-3 is built as a library which may be statistically or dynamically linked to a C++ main program. Python programs are used to import a ns3 model.

- OPNET

  It provides a comprehensive development environment supporting the modeling of communication networks and distributed systems. Both behavior and performance of modeled systems can be analyzed by performing discrete event simulations. C is a main programming language in OPNET and uses GUI for initial configurations. The simulation scenario requires C or C++.

- QualNet

  It is a commercial network simulator from Scalable Network Technologies. It is the network simulation software that predicts wireless, wired and mixed-platform network and networking device performance. A simulator for large, heterogeneous networks and the distributed applications that execute on such networks. It uses C++ for implementation of new protocols and follows a procedural paradigm.

- JSIM

  It's a java based simulator tool. It uses java and Tcl languages. It can generate new code using the source texts provided with J-Sim, compiled in the target environment compatible with JVM used.

DoS ATTACKS

Denial of Service (DoS) is a cyber-attack on an individual computer or website with intent to deny service to intended users. The purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the target machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

The attempt is to exploit various weaknesses in computer network technologies. They may target servers, networks, routers, or network communication links. Some of the DoS techniques are as follows.

- The Ping of Death attack works by generating and sending special network messages that cause problems for the systems that receive them.
- Flooding a network with useless activity so that genuine traffic cannot get through. The TCP/IP SYN and smurf attacks are two common examples.
- Remotely overloading a system's CPU so that valid requests cannot be processed.
- Changing permissions and breaking authorization logic to prevent users from logging into the system.
- Deleting or interfering with specific critical applications or services to prevent their normal operation.

DoS attacks can cause problems like ineffective services, inaccessible services, interruption of network traffic, connection interference, etc.

DDoS ATTACKS

DDoS stands for Distributed Denial of Service Attack. In DDoS attacks, the attacker tries to make a particular service unavailable by directing continuous and huge traffic from multiple end systems. Due to this enormous traffic, the network resources get utilised in serving requests of those false end systems such that a legitimate user is unable to access the resources for himself/herself.

Types of DDoS attacks –

DDoS attacks can be divided into three major categories:

1. **Application layer attacks –**

   These attacks focus on attacking the layer 7 of the OSI model where the webpages are generated in response to the request initiated by the end user. For a client, generating a request does not take any heavy load and it can easily generate multiple requests to the server. On the other hand, responding to a request takes considerable load for the server as it has to build all the pages, compute any queries and load the results from the database according to the request.

   Examples: HTTP Flood attack and attack on DNS Services. In HTTP Flood attack, multiple HTTP requests are generated simultaneously against a target server. This leads to exhaustion of network resources of that server and thus fails to serve actual users' requests. The variations of HTTP Flood attacks are – HTTP GET attack and HTTP POST attack

2. **Protocol attacks –**

   They are also known as state-exhaustion attacks. These attacks focus on vulnerabilities in the layer 3 and layer 4 of the protocol stack. These types of attacks consume resources like serves, firewalls and load balancers.

   Examples: SYN Flood attack and Ping of Death. A SYN attack exploits TCP Handshake by sending out SYN messages with a spoofed IP address. The victim server keeps on responding but does not receive final acknowledgement.

3. **Volumetric attacks –**

   Volumetric attacks focus on consuming the network bandwidth and saturating it by amplification or botnet to hinder its availability to the users. They are easy to generate by directing massive amounts of traffic to the target server.

   Examples:NTP Amplification, DNS Amplification, UDP Flood attack and TCP Flood attack. DNS Amplification works by requesting a DNS server from a spoofed IP address and structuring your request so that the DNS server responds with a large amount of data to the target victim.

ASSET MANAGEMENT AND AUDITS

The process of classifying assets requires a system or multiple systems for assigning different assets into relevant groups. These groups are devised and based on what the asset is, as well as their defining attributes. Rules are then applied to each asset group to help keep track of those particular items, which brings in an accountability structure to make the management and visibility of these items much easier to track.

An asset can be defined as any information which has some business value to the organization. It is very important for an asset classification system to be implemented, monitored and followed closely. It helps to plan and organize your devices, keep devices visible and healthy, and retire devices.

Audit means assessment and implementation of cybersecurity guidelines and standards to protect the assets. It helps the organizations to manage cyber threats. It also addresses possible risks and how to deal with it. The auditor monitors security operations and takes actions if needed. It is essential for organizations to get aware of all the risk factors and security controls.

VULNERABILITIES AND ATTACKS

A vulnerability is an inherent weakness or flaw in the design, configuration, implementation, or management of a network or system that renders it susceptible to the threat. These vulnerabilities when exposed to the threat lead to security breach. A network vulnerability could be classified as physical and non-physical. The physical network vulnerability could be resolved by protecting the physical assets like the servers. The non-physical vulnerabilities generally in the software used and the information stored.

Some of the threats to the network are malware, DoS attacks, DDoS attacks, social engineering attacks, etc.

One of the reasons for the vulnerability could also be outdated software. Developers often come out with patches to fix bugs and errors in the existing or released software. Sometimes the users are unaware of the patches or do not install them, creating a backdoor for the attackers, who will eventually gain access to the system.

Another significant threat of exposing the server or internal network to the internet could be misconfigured firewalls. Firewalls are basically a buffer area between the internet and your internal network, they filter out the content and show you only the content that is permitted by your organization. A weakly configured firewall can pose as your organization's weakness which could lead to unauthorized access to the internal network.

INTRUSION DETECTION AND PREVENTION TECHNIQUES

An intruder is often referred to as a hacker or cracker. They can be classified as follows:

• **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. A masquerader is likely to be an outsider.

• **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges. A misfeasor is an insider.

• **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. The individual can be an outsider or insider.

INTRUSION TECHNIQUES

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a backdoor into the system. Alternatively, the intruder attempts to acquire information that should have been protected. In some cases, this information is in the form of a user password.With knowledge of some other user's password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user. Each system contains a file which stores the passwords for authorized users. The password file can be protected in one of two ways:

- One-way function:The system stores only the value of a function based on the user's password.When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.

- Access control: Access to the password file is limited to one or a very few accounts.

The first and foremost goal of any system is prevention. The defender of the system should continuously monitor the system at all times to prevent any attacks. The attacker will try and find any vulnerability to get access to the system.

INTRUSION DETECTION

If the system is compromised in any way, the second way to know about it is intrusion detection. This interest is motivated by a number of considerations,including the following:

1. If the defender is able to detect any strange behavior, that is known about any sort of intrusion, then the early he gets to know the attacker would be removed earlier. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.

2. An effective intrusion detection system can serve to prevent intrusions in future.

3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of an authorized user in ways that can be detected.

Some of the approaches to intrusion detection are:

1. Statistical anomaly detection:

Involves the collection of data relating to the behavior of an authorized user over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is that of an attacker.

a. Threshold detection:

This approach involves defining thresholds, independent of the user, for the frequency of occurrence of various events.

b. Profile based:

A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

2. Rule-based detection:

Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

a. Anomaly detection:

Rules are developed to detect deviation from previous usage patterns.

b. Penetration identification:

An expert system approach that searches for suspicious behavior.

In a nutshell, statistical approaches attempt to define normal, or expected,behavior, whereas rule-based approaches attempt to define proper behavior. In terms of the types of attackers listed earlier, statistical anomaly detection is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate.On the other hand,such techniques may be unable to deal with misfeasors. For such attacks, rule-based approaches may be able to recognize events and sequences that,in context,reveal penetration.In practice, a system may exhibit a combination of both approaches to be effective against a broad range of attacks.

HOST BASED INTRUSION DETECTION SYSTEM

A host based intrusion detection system is an application that monitors a computer or network for suspicious activity, which can include intrusions by hackers as well as misuse of powers by the authorized users.

The HIDS software logs the suspicious activity and reports it to the administrators managing the devices or networks. Most applications running on devices and networks create log messages of the activities and functions performed while a session is active. If you're collecting and organizing all the various log files from all the various applications yourself, this can drain on the resources.

HIDS tools monitor the log files generated by your applications, creating a historical record of activities and functions allowing you to quickly search for them for anomalies and signs an intrusion may have occurred. The key function of HIDS tools is automated detection, which saves you the need to sort through the log files for unusual behavior once they are organized and compiled.

There are two means by which HIDSs do the actual intrusion detection on your systems: anomalies and signatures. Anomaly based detection looks for unusual or irregular activity caused by users or processes. The signature based form of detection monitors data for patterns. HIDSs running signature based detection work is similar to antivirus applications which search for bit patterns and keywords in program files by performing similar scans on log files.

SECURITY INFORMATION MANAGEMENT

Security information management (SIM) is the practice of collecting, monitoring and analyzing security-related data from computer logs. A security information management system (SIMS) automates that practice. Security information management is sometimes called security event management (SEM) or security information and event management (SIEM).

Security information includes log data generated from numerous sources, including antivirus software, intrusion detection system (IDS), intrusion prevention systems (IPS), file systems, firewalls, routers, servers and switches.

Security information management

1. Monitor events in real time.
2. Display a real time view of activity.
3. Translate event data from various sources into a common format, typically XML.
4. Aggregate data.
5. Correlate data from multiple sources.
6. Cross correlate to help administrators discern between real threats and false positives.
7. Provide automated incident response.
8. Send alerts and generate reports.

Some of the commercial SIM products are ArcSight ESM, nFX's SIM One, Network Intelligence's enVision, Prism Microsystem's EventTracker etc.

NETWORK SESSION ANALYSIS

Network session analysis is done by a Network Session Analyzer tool. NeSA is a network forensics tool to capture and analyze network traffic. Data sent through the network can be captured, recreated and exported using this tool. NeSA analyzes already captured and stored packets.

It is capable of analyzing at packet level as well as the data level. The processed information can be viewed in a multimedia display. Visualizing the data in different forms using the tool helps the analyst in analysis. It is possible to decrypt SSL sessions using NeSA, if the private key is available. Its features also include searching, filtering and packet dissection.

CHAPTER 4
CYBER SECURITY VULNERABILITIES & SAFE GUARDS

SUBTOPICS:

Internet Security, Cloud Computing & Security, Social Network sites security, Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Authorization, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, IT Audit, Authentication. Open Web Application Security Project (OWASP), Web Site Audit and Vulnerabilities assessment.

INTERNET SECURITY

Internet security is a branch of computer security which comprises various security measures exercised for ensuring the security of transactions done online. In the process, the internet security prevents attacks targeted at browsers, network, operating system and other applications. The main aim of the internet security is to set up precise rules and regulations that can deflect attacks that arise from the internet.

Internet security relies on particular resources and criteria for safeguarding the data that is communicated or transferred online. The safeguarding techniques include different kinds of encryption such as Pretty Good Privacy (PGP). Besides, the other features of a secure Web setup can include firewalls that prevent undesired traffic, and anti-spyware, anti-malware, and anti-virus programs that work from particular networks or devices to watch online traffic for malicious attachments.

Cyber Security

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

CLOUD COMPUTING AND SECURITY

Cloud computing is the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

Cloud security is a set of policies to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data and privy information of the users.

With the centralization of all company resources on cloud, the protection could be centralized. This helps in monitoring endpoints, potential threats and also threats to physical assets.

Cloud security not only reduces the costs in extra employees, loss due to attacks on physical assets. Cloud services also are able to give us a reliable environment provided all measures were taken appropriately.

SOCIAL NETWORK SITE SECURITY

Social networking is booming these days. It is popular amongst all ages, and provides promising benefits to all. But each of these applications have some vulnerability and lots of hackers are sitting there to gain benefit from it and violate privacy. Each of these networking sites consist of their own security mechanism which if not followed properly can lead to personal data or information and resource at risk thereby resulting in financial losses. In the new age, identity theft, spamming, eavesdropping, malware attacks, viruses, phishing, information leakage, etc. are threats to the privacy of people. Because of such privacy issues the interest of a lot of users turns down towards these social networking giants.

The developers should be vigilant and come up with new measures to protect the privacy of their users. Also the users should be made aware of the threats and made understand of ways to protect themselves as to falling prey to these evils of the society.

VULNERABILITIES IN SOFTWARE

Software vulnerabilities involve bugs in software. Bugs are coding errors that cause the system to make an unwanted action, vulnerabilities in short. All software has bugs of one form or another. Some bugs cause the system to crash, some cause connectivity to fail, some do not let a person to log in, etc.

Bugs are capable of all types of errors; it could be not protecting the privy information or giving access to unauthorized users. These are security vulnerabilities. It is important to consider that just about every device has software, and therefore security vulnerabilities. Operating systems, web browsers are composed of software and every other application. Even computer hardware includes a form of software called firmware. Therefore, inevitable security vulnerabilities.

In the technical media, you will hear about “buffer overflows.” Buffer overflows are forms of security vulnerabilities that frequently give a potential attacker full control of the computer. Cross-site scripting (XSS) errors are a type of coding error where a malicious party can trigger execution of software from their browser. SQL injection attacks are also an attack against websites that allow illicit access to or manipulation of the back-end databases.

You do not expect a company to knowingly release software with security vulnerabilities. Most bugs are found only after use by millions of users. Security vulnerabilities are generally found after the software has been released to the public. Some vulnerabilities might never be found, and there is no way of knowing when a vulnerability will be discovered. When a vulnerability is found, in the ideal situation, the vulnerability will be reported to the software developer, who will release a correction.

However some vulnerabilities are not properly reported and a fix/ patch isn't possible. These vulnerabilities are called zero day vulnerabilities. If the patch is available and you don't install it there are chances of your machine getting hacked.

We will operate under the assumption that a vendor does not release software knowing that there is an existing security vulnerability. We realize that this does happen, but that is a separate issue. After the software is released, in some way, the vulnerability is discovered. Once it is discovered, in the ideal world, the developer is notified of the vulnerability and can then create a patch.

If the patch is on the developers' own systems, such as a website, the problem has been successfully avoided. But if the patch involves the software in a user's computer, the vendor has to make the patch available to the end users and notify them, and then the end users have to install the patch.

The last part is where problems occur. It is very common for users, including administrators within organizations, to not implement the patches in a timely manner, if at all.

SYSTEM ADMINISTRATION

A security system administrator is someone who gives expert advice to companies regarding their internal security procedures and can also help to detect any weaknesses in a company's computer network that may make them vulnerable to cyber attacks. Security systems administrators are a company's first step in monitoring suspicious activity either within the local network or from outside internet traffic.

Security systems administrators are in charge of the daily operation of security systems, and can handle things like systems monitoring and running regular backups; setting up, deleting and maintaining individual user accounts; and developing organizational security procedures.

Computers hold a lot of valuable information that hackers would love to steal or destroy. A security systems administrator handles all aspects of information security and protects the virtual data resources of a company. They are responsible for desktop, mobile, and network security, and are also responsible for installing, administering and troubleshooting an organization's security solutions.

Security systems administrators train staff on proper protocols, monitor network traffic for any suspicious activity, perform risk assessment, audit machines and their software, update software on the latest security patches, and ensure that each network resource has the proper defenses. They can even defend against zero-day malware and in some cases, may provide evidence of a cyber attack to prosecute individuals for breaching security.

This job is based on a position of trust therefore a high sense of ethics is an important personal attribute. Detecting and neutralizing incidents is definitely part of the equation, however, being proactive and trying to implement preventative measures is most beneficial in averting security incidents.

COMPLEX NETWORK ARCHITECTURES

Network security is the set of actions adopted for prevention and monitoring of unauthorized access, ensuring information security and defense from the attacks, protection from misuses and modification of a network and its resources.

Network Security Architecture Diagram visually reflects the network's structure and construction, and all actions undertaken for ensuring the network security which can be executed with help of software resources and hardware devices, such as firewalls, antivirus programs, network monitoring tools, tools of detecting attempts of unauthorized access or intrusion, proxy servers and authentication servers.

WEAK AUTHENTICATION

Authentication refers to the process of proving an identity to an application or system. That is, the task of demonstrating that you are who you claim to be. In software systems, this usually means providing a password for a corresponding user or account identifier. While this is the most common means of proving one's identity to a system, it is not the only one.

The more difficult an authentication mechanism is to defeat the stronger it is. Clearly the authentication strength of a system should correlate to the value of the assets it is protecting. Two-Factor and Multi-Factor Authentication solutions are appropriate for systems that deal with highly valued assets.

Weak Authentication describes any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected. It also describes scenarios in which the authentication mechanism is flawed or vulnerable.

AUTHORIZATION

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources.

During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

SAFEGUARD MEASURES

ACCESS CONTROL

Access control is a security technique that regulates who or what can view or use resources in an environment. It is the basic method of protecting the system from misuse.

User authentication is necessary to control access to the network systems, in particular network infrastructure devices. Authentication has two aspects: general access authentication and functional authorization.

General access authentication is the method to control whether a particular user has any type of access right to the system he is trying to connect to. User authentication depends on the correct authentication. The use of more than one factor for identification and authentication provides the basis for Multi Factor authentication.

At a minimum level, all network devices should have username-password authentication. The password should be non-trivial (at least 10 characters, mixed alphabets, numbers, and symbols).

In case of remote access by the user, a method should be used to ensure usernames and passwords are not passed in the clear over the network. Also, passwords should also be changed with some reasonable frequency.

IT AUDIT

An IT audit is the examination and evaluation of an organization's information, technology, infrastructure and policies. Based on the result of the evaluation, it is determined whether the assets are safeguarded satisfactorily and the CIA triad is fulfilled.

The audit process includes the following steps or phases:

1. Planning.
2. Definition of audit objectives and scope.
3. Evidence collection and evaluation.
4. Documentation and reporting.

OPEN WEB APPLICATION SECURITY PROJECT(OWASP)

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks. The report is put together by a team of security experts from all over the world. OWASP refers to the Top 10 as an 'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.

Below are the security risks reported in the OWASP Top 10 2017 report:

1. Injection

A. Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application.
B. Injection attacks can be prevented by validating and/or sanitizing user-submitted data. (Validation means rejecting suspicious-looking data, while sanitization refers to cleaning up the suspicious-looking

parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.

2. Broken Authentication

A. Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account.
B. Some strategies to mitigate authentication vulnerabilities are requiring 2-factor authentication (2FA) as well as limiting or delaying repeated login attempts using rate limiting.

3. Sensitive Data Exposure

A. If web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and sell or utilize it for nefarious purposes. One popular method for stealing sensitive information is using a man-in-the-middle attack.
B. Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching* of any sensitive information. Additionally, web application developers should take care to ensure that they are not unnecessarily storing any sensitive data.

4. XML External Entities (XEE)

A. This is an attack against a web application that parses XML input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.
B. The best ways to prevent attacks are to have web applications accept a less complex type of data, such as JSON, or at the very least to patch XML parsers and disable the use of external entities in an XML application.

5. Broken Access Control

A. Access control refers to a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators.
B. Access controls can be secured by ensuring that a web application uses authorization tokens and sets tight controls on them.

6. Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors.

7. Cross-Site Scripting

A. Cross-site scripting vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users. This vulnerability can be exploited to run malicious JavaScript code on a victim's browser.
B. Mitigation strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and/or sanitizing user-generated content. Using modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.

8. Insecure Deserialization

A. This threat targets the many web applications which frequently serialize and deserialize data. Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it. Deserialization is just the opposite: converting serialized data back into objects the application can use. Serialization is sort of like packing furniture away into boxes before a move, and

deserialization is like unpacking the boxes and assembling the furniture after the move. An insecure deserialization attack is like having the movers tamper with the contents of the boxes before they are unpacked.

B. An insecure deserialization exploit is the result of deserializing data from untrusted sources, and can result in serious consequences like DDoS attacks and remote code execution attacks. While steps can be taken to try and catch attackers, such as monitoring deserialization and implementing type checks, the only sure way to protect against insecure deserialization attacks is to prohibit the deserialization of data from untrusted sources.

9. Using Components With Known Vulnerabilities

A. Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common examples include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks. Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.

B. Component developers often offer security patches and updates to plug up known vulnerabilities, but web application developers don't always have the patched or most-recent versions of components running on their applications. To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.

10. Insufficient Logging And Monitoring

Many web applications are not taking enough steps to detect data breaches. The average discovery time for a breach is around 200 days after it has happened. This gives attackers a lot of time to cause damage before there is any response. OWASP recommends that web developers should implement logging and monitoring as well as incident response plans to ensure that they are made aware of attacks on their applications.

WEBSITE AUDIT

A website audit is the analysis of a site looking at the factors that determine visibility in Google.An audit gives you insight into the performance of the website as a whole. This gives you an understanding of any issues and where to concentrate your efforts. The in-depth examination of the website requires experience to understand the potential opportunities.

An audit is also the key step before you complete any major changes on your websites such as a refresh, migration or a full overhaul, it can serve as a marker so that you know when something went wrong and how long it's been going wrong.

VULNERABILITY ASSESSMENT

A vulnerability assessment is a risk management process used to identify, quantify and rank possible vulnerabilities to threats in a given system. It is not isolated to a single field and is applied to systems across different industries, such as:

- IT systems
- Energy and other utility systems
- Transportation
- Communication systems

The key component of a vulnerability assessment is the proper definition for impact loss rating and the system's vulnerability to that specific threat. Impact loss differs per system.

Vulnerability assessments are designed to yield a ranked or prioritized list of a system's vulnerabilities for various kinds of threats. Organizations that use these assessments are aware of security risks and understand they need help identifying and prioritizing potential issues. By understanding their vulnerabilities, an organization can formulate solutions and patches for those vulnerabilities for incorporation with their risk management system.

CHAPTER 5
MALWARE

SUBTOPICS:

Explanation of Malware, Types of Malware: Virus, Worms, Trojans, Rootkits, Robots, Adware's, Spywares, Ransom wares, Zombies etc., OS Hardening (Process Management, Memory Management, Task Management, Windows Registry/ services another configuration), Malware Analysis.

WHAT IS MALWARE?

A malware or malicious software consists of a computer program specifically developed to cause damage to data and systems on the user's computer or to gain unauthorized access to a network. Malware is distributed in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

A software is identified as a malware based on its intended use, rather than a particular technique or technology used to build it.

TYPES OF MALWARE

WORM:

A worm is a computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network. The first ever worm that was created was nonmalicious, searching for idle systems to use to run a computationally intensive task.

Once active within a system, a network worm can behave as a computer virus or bacteria,or it could implant Trojan horse programs or perform any number of disruptive or destructive actions. To replicate itself, a network worm uses some sort of network vehicle. Examples include the following:

• Electronic mail facility:

A worm mails a copy of itself to other systems,so that its code is run when the e-mail or an attachment is received or viewed.

• Remote execution capability:

A worm executes a copy of itself on another system, either using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations.

• Remote login capability:

A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes.

A network worm exhibits the same characteristics as a computer virus: a dormant phase,a propagation phase,a triggering phase,and an execution phase.The propagation phase generally performs the following functions:

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.

2. Establish a connection with a remote system.

3. Copy itself to the remote system and cause the copy to be run.

The network worm may also attempt to determine whether a system has previously been infected before copying itself to the system.In a multiprogramming system,it may also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator.

WORM COUNTERMEASURES:

1. Generality: The approach taken should be able to handle a wide variety of worm attacks,including polymorphic worms.
2. Timeliness: The approach should respond quickly so as to limit the number of infected systems and the number of generated transmissions from infected systems.
3. Resiliency: The approach should be resistant to evasion techniques employed by attackers to evade worm countermeasures.
4. Minimal denial-of-service costs:The approach should result in minimal reduction in capacity or service due to the actions of the countermeasure software. That is, in an attempt to contain worm propagation, the countermeasure should not significantly disrupt normal operation.
5. Transparency: The countermeasure software and devices should not require modification to existing (legacy) OSs,application software,and hardware.
6. Global and local coverage: The approach should be able to deal with attack sources both from outside and inside the enterprise network.

VIRUS:

A computer virus is a piece of software that can “infect”other programs by modifying them;the modification includes injecting the original program with a routine to make copies of the virus program,which can then go on to infect other programs.Computer viruses first appeared in the early 1980s,and the term itself is attributed to Fred Cohen in 1983.

A computer virus carries in its instructional code the recipe for making perfect copies of itself.The typical virus becomes embedded in a program on a computer.Then, whenever the infected computer comes into contact with an uninfected piece of software,a fresh copy of the virus passes into the new program.Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network. In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.

A computer virus has three parts:

• Infection mechanism: The means by which a virus spreads,enabling it to replicate.The mechanism is also referred to as the infection vector.

• Trigger: The event or condition that determines when the payload is activated or delivered.

• Payload: What the virus does, besides spreading.The payload may involve damage or may involve benign but noticeable activity.

During its lifetime,a typical virus goes through the following four phases:

• Dormant phase:

The virus is idle.The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.Not all viruses have this stage.

• Propagation phase:The virus places a copy of itself into other programs or into certain system areas on the disk.The copy may not be identical to the propagating version;viruses often morph to evade detection.Each infected program will now contain a clone of the virus,which will itself enter a propagation phase.

• Triggering phase: The virus is activated to perform the function for which it was intended.As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies itself.

• Execution phase: The function is performed.The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

VIRUS CLASSIFICATION

A virus classification by target includes the following categories:

• Boot sector infector: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

• File infector: Infects files that the operating system or shell considers to be executable.

• Macro virus: Infects files with macro code that is interpreted by an application.

A virus classification by concealment strategy includes the following categories:

• **Encrypted virus:** A typical approach is as follows.A portion of the virus creates a random encryption key and encrypts the remainder of the virus.The key is stored with the virus.When an infected program is invoked, the virus uses the stored random key to decrypt the virus.When the virus replicates,a different random key is selected. Because the bulk of the virus is encrypted with a different key for each instance,there is no constant bit pattern to observe.

• **Stealth virus:** A form of virus explicitly designed to hide itself from detection by antivirus software.Thus,the entire virus,not just a payload is hidden.

• **Polymorphic virus:** A virus that mutates with every infection, making detection by the "signature"of the virus impossible.

• **Metamorphic virus:**As with a polymorphic virus,a metamorphic virus mutates with every infection.The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

VIRUS KITS

Another weapon in the virus writers' armory is the virus-creation toolkit. Such a toolkit enables a relative novice to quickly create a number of different viruses. Although viruses created with toolkits tend to be less sophisticated than viruses designed from scratch,the sheer number of new viruses that can be generated using a toolkit creates a problem for antivirus schemes.

TROJANS:

A Trojan horse is a useful, or apparently useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function. Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.

Another common motivation for the Trojan horse is data destruction.The program appears to be performing a useful function (e.g.,a calculator program),but it may also be quietly deleting the user's files. For example, a CBS executive was victimized by a Trojan horse that destroyed all information contained in his computer's memory. The Trojan horse was implanted in a graphics routine offered on an electronic bulletin board system. Trojan horses fit into one of three models:

- Continuing to perform the function of the original program and additionally performing a separate malicious activity.
- Continuing to perform the function of the original program but modifying the function to perform malicious activity (e.g., a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity (e.g.,a Trojan horse version of a process listing program that does not display certain processes that are malicious).
- Performing a malicious function that completely replaces the function of the original program

SPYWARE:

It is the malware used for the purpose of secretly gathering data on an unsuspecting user. It spies on the behaviour of the user of the computer, and on the data you send and receive, usually with the purpose of transmitting this data to another system. A keylogger is a specific kind of spyware that records all the keystrokes a user makes, a great tool for stealing passwords.

ROOTKIT:

A rootkit is a program or collection of software tools that gives a threat actor remote access to and control over a computer or other system. It gets its name as it is a kit of tools that gains root access over the target system, and uses the power to hide their presence.

ADWARE:

Adware is a malware that forces your browser to redirect to web advertisements, which often themselves seek to download further, even more malicious software.

RANSOMWARE:

Ransome is the malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The payment to cybercriminals is usually in bitcoin. It is achieved by phishing and social engineering.

ZOMBIE/ BOT:

It is a program activated on an infected machine that is activated to launch attacks on other machines.

BACKDOOR:

A trapdoor or backdoor is any mechanism that bypasses a normal security check;it may allow unauthorized access to functionality.

OS HARDENING

The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications.

Advanced system hardening may involve reformatting the hard disk and only installing the bare necessities that the computer needs to function. The CD drive is listed as the first boot device, which enables the computer to start from a CD or DVD if needed. File and print sharing is turned off if not absolutely necessary and TCP/IP is often the only protocol installed. The guest account is disabled, the administrator account is renamed, and secure passwords are created for all user logins. Auditing is enabled to monitor unauthorized access attempts.

While these steps are often part of operating system hardening, system administrators may choose to perform other tasks that boost system security.

MALWARE ANALYSIS

Malware analysis is the process of learning how malware functions and any potential repercussions of a given malware. Malware code caan differ radically, and it's essential to know that malware can have many functionalities. These may come in the form of viruses, worms and trojan horses. Each type of malware gathers information about the infected device without the knowledge, or authorization of the user.

STAGES OF MALWARE ANALYSIS

Investigating malware is a process that requires taking a few steps. These four stages form a pyramid that grows in intricacy. The closer you get to the top of the pyramid, the stages increase in complexity and the skills needed to implement them are less common. Here we start from the bottom:

1. **Fully automated analysis:**

   One of the simplest ways to assess a suspicious program is to scan it with fully automated tools. Fully automated tools are able to quickly assess what a malware is capable of if it infiltrates the system. This analysis is able to produce a detailed report regarding the network traffic, file activity, and registry keys. Even though a fully automated analysis does not provide as much information as an analyst, it is still the fastest method to sift through large quantities of malware.

2. **Static properties analysis:**

   In order to get a more in depth look at malware, it is imperative to look at its static properties. It is easy to access these properties because it does not require running the potential malware, which takes a longer time. The static properties include hashes, embedded strings, embedded resources, and the header information. The

properties should be able to show elementary indicators of compromise.

3. Interactive behavior analysis:

To observe a malicious file, it might oftentimes be put in an isolated laboratory to see if it directly infects the laboratory. Analysts will frequently monitor these laboratories to see if the malicious file tries to attach to any hosts. With this information, the analyst will then be able to replicate the situation to see what the malicious file would do once it was connected to the host, giving them an advantage over those who use automated tools.

4. Manual code reversing:

Reversing the code of the malicious file can decode encrypted data that was stored by the sample, determine the logic of the file's domain, and see other capabilities of the file that did not show up during the behavioral analysis. In order to manually reverse the code, malware analysis tools such as a debugger and disassembler are needed. The skills needed to complete manual code reversing are very important, but also difficult to find.

CHAPTER 6
SECURITY IN EVOLVING TECHNOLOGY

SUBTOPICS:

Biometrics, Mobile Computing and Hardening on android and ios, IOT Security, Web server configuration and Security. Introduction, Basic security for HTTP Applications and Services, Basic Security for Web Services like SOAP, REST etc., Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

BIOMETRICS

Biometrics is the measurement and statistical analysis of people's unique physical and behavioural characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioural traits.

Components of biometric devices include:

1. A reader or scanning device to record the biometric factor being authenticated.
2. Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with the stored data.
3. A database to securely store biometric data for comparison.

Biometric implementations depend on gathering biometric data locally and then cryptographically hashing it so that authentication or

identification can be accomplished without direct access to the biometric data itself.

Biometric identifiers depend on either physiological or behavioural characteristics. Physiological identifiers relate to the composition of the user being authenticated and include facial recognition, fingerprints, finger geometry, iris recognition, vein recognition, retina scanning, voice recognition and DNA matching. Behavioural identifiers include the unique ways in which individuals act, including recognition of typing patterns, walking gait and other gestures. Some of these behavioural identifiers can be used to provide continuous authentication instead of a single one-off authentication check.

Biometric identifiers depend on the uniqueness of the factor being considered. Other biometric factors, including etina, iris, vein and voice scans, have not been adopted widely so far, in some part because there is less confidence in the uniqueness of the identifiers or because the factors are easier to spoof.

Stability of the biometric factor can also be important to acceptance of the factor. Fingerprints do not change over lifetime, while facial appearance can change drastically with age and other factors. The most significant privacy issue of using biometrics is that physical attributes like fingerprints and retinal blood vessel patterns are generally static and cannot be modified. This is in distinction to nonbiometric factors like passwords and tokens, which can be replaced if they are breached or otherwise compromised.

The increasing ubiquity of high-quality cameras, microphones and fingerprint readers in many of today's mobile devices means biometrics will continue to become a more common method for authenticating users, particularly as Fast ID Online (FIDO) has specified new standards for authentication with biometrics that support two-factor authentication with

biometric factors.

While the quality of biometric readers continues to improve, they can still produce false negatives, when an authorized user is not recognized or authenticated, and false positives, when an unauthorized user is recognized and authenticated.

While high quality cameras and other sensors help enable the use of biometrics, they can also enable attackers. Because people do not shield their faces, ears, hands, voice or gait, attacks are possible simply by capturing biometric data from people without their consent or knowledge.

MOBILE COMPUTING AND HARDENING ON ANDROID AND IOS

Hardening is a key step at the end of any secure software development life cycle process, which ensures that the app is running as designed at runtime and thwarts cybercriminal's efforts to reverse engineer the app back to source code.

Below are four key factors that those responsible for app security should consider when evaluating application hardening solutions.

1. The value of your app:

An important factor to consider is the level of investment your company is making in an app with respect to research and development and maintenance costs.

If the app will be processing sensitive information such as financial transactions, account information or authorization credentials, you should consider the potential loss of revenue through fraud and collateral damage that may accrue if the app is hacked or Trojanized. Collateral damage may include not only penalties for noncompliance with regulations and necessary expenditures on security upgrades, but also the costs of crisis management communication campaigns to manage adverse publicity and restore brand value.

2. The scale and sophistication of attacks your app will likely face:

Minimal protections against counterfeiting and repackaging are built into the app distribution ecosystem. These include measures such as:

- The detection of jailbreak or root conditions that enable the side-loading of applications, many of which are Trojanized;
- Monetization libraries that ensure only legitimate applications are downloaded through the app store and are correctly purchased or licensed. However, these libraries can and are often breached by cybercriminals; and
- Audit process measures to ensure only legitimate and harmless apps are placed in the app store, even though audit mechanisms to block illegitimate apps from distribution to users are far from perfect.

3. Agility and Portability:

Mobile platforms will continue to evolve at their current breakneck pace, choosing a solid security partner with a history of innovation and keeping pace with ecosystem changes is crucial. Additionally, selecting a security tool that is designed for cross-platform portability and extensibility will go a long way toward ensuring that your ability to reach out to the newest platforms is not hindered in any way.

4. Overhead and Performance Impact:

Memory footprint, power consumption and performance are important considerations on portable devices where resources are limited and battery life is precious. Any security technology will

impose an additional memory footprint in storage and at runtime. It will also impose process overhead in terms of programming effort, compilation complexity and runtime execution characteristics.

That said, more sophisticated application hardening solutions offer a much better trade-off between performance impact and protection strength relative to free or low cost solutions.

When apps will be deployed to millions of users, or where transaction volumes are expected to be high, it is crucial that the security solution chosen be as robust and reliable as your own app code.

The rise of mobile computing and soaring app usage has companies of every size scrambling to keep up. With customer loyalty and revenues at stake, developers are often rushing to release cutting-edge apps with little thought for long-term security considerations.

IOT SECURITY

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken.

IoT security is the technology area concerned with safeguarding connected devices and networks in the internet.Your connected devices are data collectors. The personal information collected and stored with these devices — such as your name, age, health data, location and more — can aid criminals in stealing your identity.At the same time, the Internet of Things is a growing trend, with a stream of new products hitting the market. But here's the problem: When you're connected to everything, there are more ways to access your information. That can make you an attractive target for people who want to make a profit off of your personal data. Some of the ways to protect your IoT devices are:

1. Install reputable internet security software on your computers, tablets, and smartphones.
2. Use strong and unique passwords for device accounts, Wi-Fi networks, and connected devices.
3. Always read the privacy policy of the apps you use to see how they plan on using information and more.
4. Devices become smart because they collect a lot of personal data. While collecting data isn't necessarily a bad thing, you

should know about what types of data these devices collect, how it's stored and protected, if it is shared with third parties, and the policies or protections regarding data breaches.

5. Know what data the device or app wants to access on your phone. If it seems unnecessary for the app's functionality or too risky, deny permission.
6. Use a VPN, like Norton Secure VPN, which helps to secure the data transmitted on your home or public Wi-Fi.
7. Check the device manufacturer's website regularly for firmware updates.
8. Use caution when using social sharing features with these apps. Social sharing features can expose information like your location and let people know when you're not at home. Cybercriminals can use this to track your movements.
9. Never leave your smartphone unattended if you're using it in a public space. In crowded spaces, you should also consider turning off Wi-Fi or Bluetooth access if you don't need them. Some smartphone brands allow automatic sharing with other users in close proximity.

WEB SERVER CONFIGURATION AND SECURITY

A web server is software or hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond. There are four leading web servers - Apache, IIS, lighttpd and Jigsaw. Some of the expensive ones are Netscape's iPlanet, Bea's Web Logic and IBM's WebSphere.

Web server security is the protection of information assets that can be accessed from a web server. Web server security is important for any organization that has a physical or virtual Web server connected to the Internet. It requires a layered defense and is especially important for organizations with customer-facing websites.

Separate servers should be used for internal and external-facing applications and servers for external-facing applications should be hosted on a DMZ or containerized service network to prevent an attacker from exploiting a vulnerability to gain access to sensitive internal information.

Penetration tests should be run on a regular basis to identify potential attack vectors, which are often caused by out-of-date server modules, configuration or coding errors and poor patch management. Web site security logs should be audited on a continuous basis and stored in a secure location. Other best practices include using a separate development server for testing and debugging, limiting the number of superuser and administrator accounts and deploying an intrusion detection system (IDS) that includes monitoring and analysis of user and system activities, the recognition of patterns typical of attacks, and the analysis of abnormal activity patterns.

CHAPTER 7
CYBER LAWS AND FORENSICS

SUBTOPICS:

Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013. Introduction to Cyber Forensics, Need of Cyber Forensics, Cyber Evidence, Documentation and Management of Crime Sense, Image Capturing and its importance, Partial Volume Image, Web Attack Investigations, Denial of Service Investigations, Internet Crime Investigations, Internet Forensics, Steps for Investigating Internet Crime, Email Crime Investigations

INTRODUCTION

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law is referred to as the Law of the Internet.

Like any law, a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

CYBER SECURITY REGULATIONS

A cybersecurity regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyberattacks like viruses, worms, trojan horses, phishing, denial of service attacks, unauthorized access and control system attacks. There are numerous measures available to prevent cyberattacks.

Cybersecurity measures include firewalls, anti-virus software, intrusion detection and prevention systems, encryption, and login passwords. There have been attempts to improve cybersecurity through regulation and collaborative efforts between the government and the private sector to encourage voluntary improvements to cybersecurity. Industry regulators, including banking regulators, have taken notice of the risk from cybersecurity and have either begun or planned to begin to include cybersecurity as an aspect of regulatory examinations.

NATIONAL CYBER SECURITY POLICY 2013

It is a policy framework by the Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyber attacks. The policy also intends to safeguard information, such as personal information, financial and banking information and sovereign data.

India had no cyber security policy before 2013. **The reason for cyber security is to build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in your privacy and to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.**

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).

- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.

- To enhance and create National and Sectoral level 24X7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

CYBER FORENSICS

The process of gathering and documenting proof from a computer or a computing device in a form presentable to the court by applying the techniques of investigation and analysis is called Cyber Forensics. Cyber Forensics is also called Computer Forensics.

The aim of cyber forensics is to determine who is responsible for what exactly happened on the computer while documenting the evidence and performing a proper investigation. The storage media of the device under investigation is made into a digital copy by the investigators and the investigation is performed on the digital copy while making sure the device under investigation is not contaminated accidentally.

NEED OF CYBER FORENSICS

There are cases like hacking and denial of service (DOS) attacks where the computer system is the crime scene. The proof of the crime will be present in the computer system. The proof can be browsing history, emails, documents, etc. These proofs on the computer system alone can be used as evidence in the court of law to sort out allegations or to protect innocent people from charges.

CYBER EVIDENCE

Cyber evidence is any information about the crime scene, it can be from a digital media like computer, mobile phone, server or network. For solving the crimes committed on digital materials, they have to be copied. Evidence must be copied properly in valid methods that provide legal availability. Otherwise, the material cannot be used as evidence. There are different types of digital forensics to extract information:

Disk Forensics:

It deals with extracting data from storage media by searching active, modified, or deleted files.

Network Forensics:

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

Wireless Forensics:

It is a division of network forensics. The main aim of wireless forensics is to offer the tools needed to collect and analyze the data from wireless network traffic.

Database Forensics:

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

Malware Forensics:

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Email Forensics

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

Memory Forensics:

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

Mobile Phone Forensics:

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

DOCUMENTATION AND MANAGEMENT OF CRIME SENSE

In documentation, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

The purpose of crime scene management is to control, preserve, record, and recover evidence from the scene of an incident. Any evidence removed from a scene by investigators must be packaged and labeled correctly to prevent injury and contamination. Once forensic analysis begins, it is important to ensure that the questions asked are investigative and not purely scientific. It is sometimes useful to bring the forensic specialist to the crime scene itself.

1. As law enforcement officers at a physical crime scene first scan the area to make initial observations about how the incident occurred, security professionals must first assess the business impact of a technological crime scene. Specifically, they must determine the incident's severity, whether confidential information was compromised, what steps have been taken to contain the immediate threat and how the attack happened. Shutting down a system too quickly could compromise a forensic investigation. Therefore, security professionals should quickly identify what systems or servers have been affected, what data could be lost if a computer or system is powered off and what static data is stored on hard drives.

2. Similar to taking photographs and fingerprints at a physical crime scene, security professionals should use forensic imaging to record the affected system and related components. That approach captures significant network traffic and creates a snapshot of the network at the time the incident occurred. If system changes are made later in the investigation, an exact image of the breached network is preserved for analysis.
3. Next, the investigators should evaluate all available information sources, including virtual machines, log files and external devices that might have been used. They should “fingerprint” physical evidence using a one-way hash -- a cryptographically sound, non-reversible algorithm that becomes unique to the source being collected and can easily be verified later to prove the integrity of collected information.
4. If a cyber crime eventually proceeds to trial, a thorough report of the steps taken during the breach investigation will be important for the prosecution. To better defend any challenge to statements of fact made in the account, security professionals should include information on how the analyzed artifacts were recovered from collected data.

IMAGE CAPTURING AND IMPORTANCE

Image acquisition of the materials from the crime scene by using the proper hardware and software tools makes the obtained data legal evidence. Choosing the proper format and verification function when image acquisition affects the steps in the research process. For this purpose, investigators use hardware and software tools.

Hardware tools assure the integrity and trueness of the image through a write-protected method. As for software tools, they provide usage of certain write-protect hardware tools or acquisition of the disks that are directly linked to a computer. Image acquisition through writeprotect hardware tools assures them the feature of forensic copy. Image acquisition only through software tools does not ensure the forensic copy feature. During the image acquisition process, different formats like E01, AFF, DD can be chosen.

In order to provide the integrity and trueness of the copy, hash values have to be calculated using verification functions like SHA and MD series. In this study, image acquisition processes through hardware-software are shown. Hardware acquisition of a 200 GB capacity hard disk is made through Tableau TD3 and CRU Ditto. The images of the same storage are taken through Tableau, CRU and RTX USB bridge and through FTK imager and Forensic Imager.

INTERNET FORENSICS

Forensics is the application of scientific methods in criminal investigations. Computer forensics studies how computers are involved in the commission of crimes. In cases ranging from accounting fraud, to blackmail, identity theft, and child pornography, the contents of a hard drive can contain critical evidence of a crime. The analysis of disks and the tracking of emails between individuals have become commonplace tools for law enforcement around the world.

Internet forensics shifts that focus from an individual machine to the Internet at large. With a single massive network that spans the globe, the challenge of identifying criminal activity and the people behind it becomes immense.

STEPS OF INVESTIGATING INTERNET CRIME

1. BACKGROUND CHECK:

   To establish a starting point in a crime scene, defining the background with known facts is important.

2. INFORMATION GATHERING:

   To check if the attacker was a human or a robot. To find out which type of attack was performed and other details that could point out to the reasons behind the crime and the person behind it.

3. TRACKING AND IDENTIFYING THE CRIMINALS.
4. DIGITAL FORENSICS.

EMAIL FORENSICS

Studying the source and content of electronic mail as evidence, identifying the actual sender and recipient of a message and the physical location from which it was sent through email routing, as well as finding out the date/time etc. Another part of email forensics is the investigation of lost emails, i.e. at what point was an email interrupted on it's route (blacklisting, spam filters etc.).

Investigating email crimes is the process of tracing, collecting, analyzing and investigating digital evidence and cyber traits. Digital evidence and cyber traits can relate to email spamming, mail bombing/mail storms, email spoofing, identity fraud, phishing attacks and email hijacking.

The primary evidence in email investigations is the email header. The email header contains a considerable amount of information about the email. Email header analysis should start from bottom to top, because the bottom-most information is from the sender, and the top-most information is about the receiver.

Header Analysis

Email header analysis is the primary analytical technique. This involves analyzing metadata in the email header. It is evident that analyzing headers helps to identify the majority of email-related crimes. Email spoofing, phishing, spam, scams and even internal data leakages can be identified by analyzing the header.

Server Investigation

This involves investigating copies of delivered emails and server logs. In some organizations they do provide separate email boxes for their employees by having internal mail servers. In this case,

investigation involves the extraction of the entire email box related to the case and the server logs.

Network Device Investigation

In some investigations, the investigator requires the logs maintained by the network devices such as routers, firewalls and switches to investigate the source of an email message. This is often a complex situation where the primary evidence is not percent.

Software Embedded Analysis

Some information about the sender of the email, attached files or documents may be included with the message by the email software used by the sender for composing the email. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF).

Sender Mail Fingerprints

The "Received" field includes tracking information generated by mail servers that have previously handled a message, in reverse order. The "X-Mailer" or "User-Agent" field helps to identify email software. Analyzing these fields helps to understand the software, and the version used by the sender.

Use of Email Trackers

In some situations, attackers use different techniques and locations to generate emails. In such situations it is important to find out the geographical location of the attacker. To get the exact location of the attacker, investigators often use email tracking software embedded into the body of an email. When a recipient opens a message that has an email tracker attached, the investigator will be notified with the IP address and geographical location of the

recipient. This technique is often used to identify suspects in murder or kidnapping cases, where the criminal communicates via email.

Volatile Memory Analysis

Recent research has been conducted in analyzing spoofed emails from volatile memory. Since everything passes through volatile memory, it is possible to extract email related evidence (header information) from volatile memory.

Attachment Analysis

Most viruses and malware are sent through email attachments. Investigating attachments is crucial in any email-related investigation. Confidential information leakage is another important field of investigation. There are software tools available to recover email-related data, such as attachments from computer hard discs. For the analysis of suspicious attachments, investigators can upload documents into an online sandbox such as VirusTotal to check whether the file is malware or not.