Introduction to Cyber Security

Md. Masud Rana
Lecturer,
Department of Cyber Security Engineering (CySE)

1.1 Introduction to Cyber Security

1.1.1 Cyber: Cyber is a prefix that denotes a relationship with information technology (IT). IT is a set of related fields that encompass computer systems, software, programming languages, and data and information processing, and storage. Anything relating to computing, such as the internet, falls under the cyber category. i.e. Cyberspace, Cybersecurity, Cybercrime, Cyberattack, Cyberbullying, Cyberforensics.

1.1.2 Security: Security is protection from, or resilience against, potential harm (or other unwanted coercion). Beneficiaries (technically referents) of security may be persons and social groups, objects and institutions, ecosystems, or any other entity or phenomenon vulnerable to unwanted change.

1.1.3 Cyber Security:

Cybersecurity refers to any technologies, practices and policies for preventing cyberattacks/Cybercrime or mitigating their impact. Cybersecurity aims to protect computer systems, applications, devices, data, financial assets and people against cyberthreats. Comprehensive cybersecurity strategies protect all of an organization’s IT infrastructure layers against cyberthreats and cybercrime. Some of the most important cybersecurity domains include:

- AI security
- Critical infrastructure security
- Network security
- Endpoint security
- Application security
- Cloud security
- Information security
- Mobile security

1.1.4 The 3 Pillars of Cyber Security

- **People**: People are the key components to consider when you administer and protect a company or individual’s assets. They help drive the cyber security process, from multiple angles. They include decision makers, like C-suite executives, directors, and management; they also include the people who implement cyber security, like staff and third-party consultants.
- **Process**: Processes and policy help provide the framework for governance and also define procedures that can be measured over time. Processes inform an IT department’s preventative and responsive controls. This means processes are put into place to support the integrity of a security system. For example, a separation

of duties ensures no single person is responsible for signing off on changes made to a product or system. Similarly, physical barriers like secure spaces, can ensure access and safety to hardware. Detective controls like regular audits and reviews make sure you follow best practices and handle software and data securely.

- **Technology**: Technology is the hardware and software that departments use to achieve reliable cyber security. They are the mechanisms IT people build processes around to prevent compromises to an IT infrastructure. They might include behavior analytics that monitor user or staff behavior or transactions. It might be breach detection which notifies you of hackers or malware. Or an authentication response system which confirm a user's credentials. These technologies can be layered to create a fortified system that makes it difficult for a cyber threat to infiltrate private data.

1.1.5 Goals of Cyber Security

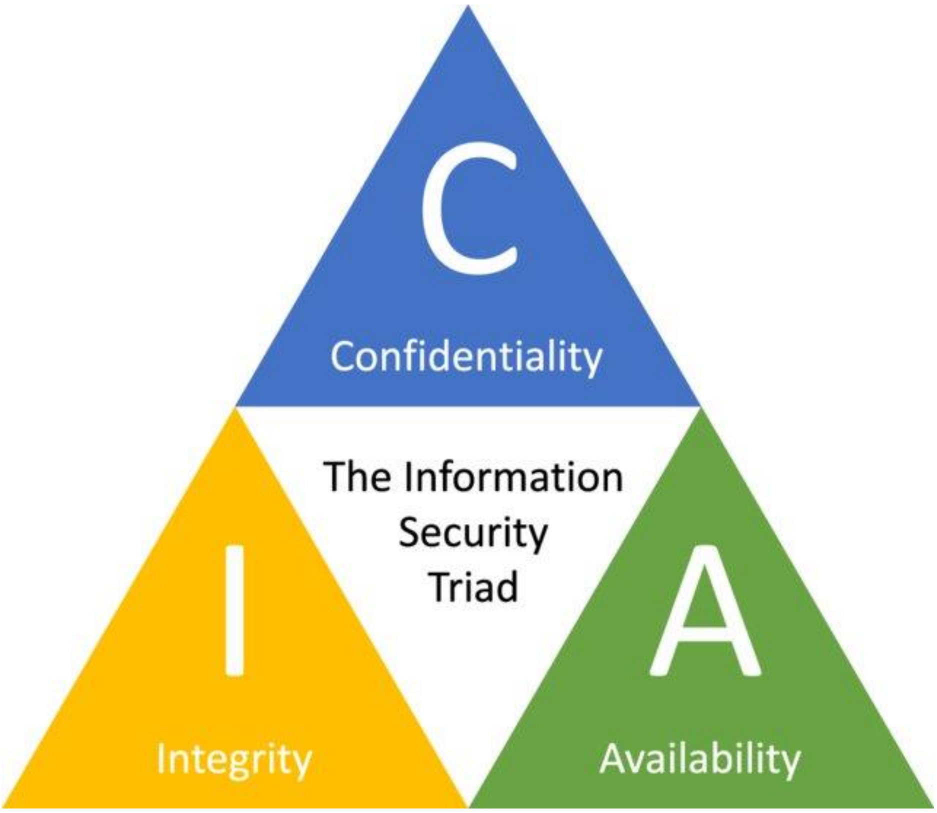


Fig: CIA Triad

Confidentiality protects information (data) from unauthorized access. To solve:

1. **Encrypt sensitive data**, such as credit card numbers or personal information, when you transmit it over networks or store it on computers.
2. **Use access controls**, such as user authentication and authorization, to limit who can access sensitive data and what they can do with it.

3. **Use physical controls**, such as locks and security cameras, to prevent unauthorized access to sensitive data in physical locations, such as data centers or office buildings.
4. **Maintain a clear data protection policy and regularly train employees** on security best practices to teach them how to handle sensitive information properly.

Integrity is the accuracy and consistency of data as well as the completeness and reliability of systems. A breach of integrity occurs when there's a change in data. This can happen in various ways:

1. **Data corruption** might occur when a software bug or hardware malfunction causes wrong transmission and storage of data, resulting in errors or inconsistencies.
2. **Malicious software.** When an attacker injects malicious software, such as a virus into the system, the virus might change data without the user's knowledge or consent, potentially causing damage or disruption.
3. **Tampering** refers to an unauthorized user physically accessing a computer or storage device and changing the data on it, either by deleting or altering the data or by adding false or misleading information.

Businesses can use checksums or cryptographic hashes to verify that data isn't changed or corrupted. Additionally, they can use transaction logs or audit trails to track changes to data and systems so they can detect and correct any unauthorized or improper changes.

Availability is the ability for users to access systems and information when needed, even under duress. Ensuring availability must be baked into many areas of network and software development:

- **Deploy redundant systems** such as multiple servers or backup power sources or implement caching. This way, when one system fails, the others can continue to operate and provide the data you need.
- **Use load balancers**, which distribute incoming requests across multiple systems so that no single system becomes overwhelmed and unavailable.
- **Regularly test and maintain your systems** to help identify and address potential availability issues before they cause disruptions.

1.2 Cyber Crime/ Cyber Attack

The term **cyber crime** is used to describe an unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants (PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often committed by the people of destructive and criminal mindset either for revenge, greed or adventure.

1.2.1 Classification of Cyber Crimes

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

- *Insider Attack:* An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when an employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vulnerability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.
- *External Attack:* When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analyzing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker.

- *Unstructured attacks:* These attacks are generally performed by amateurs who don’t have any predefined motives to perform the cyber attack. Usually these amateurs try to test a tool readily available over the internet on the network of a random company.

- *Structure Attack:* These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems (IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

1.2.2 Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

a. *Money:* People are motivated towards committing cyber crime is to make quick and easy money.

b. *Revenge:* Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.

c. *Fun:* The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.

d. *Recognition:* It is considered to be pride if someone hack the highly secured networks like defense sites or networks.

e. *Anonymity*- Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.

f. *Cyber Espionage:* At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

1.3 MALWARE AND ITS TYPE

Malware stands for "*Malicious Software*" and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

1.3.1 Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

1.3.2 Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programs from the internet. Spywares may be of various types; It can keep track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

1.3.3 Browser hijacking software

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

1.3.4 Virus

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention.

Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

1.3.5 Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they do not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consume the network resources like space and bandwidth and force the network to choke.

1.3.6 Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of *botnet (*ro*bot-net*work*)*, a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojans neither infect the other computers in the network nor do they replicate.

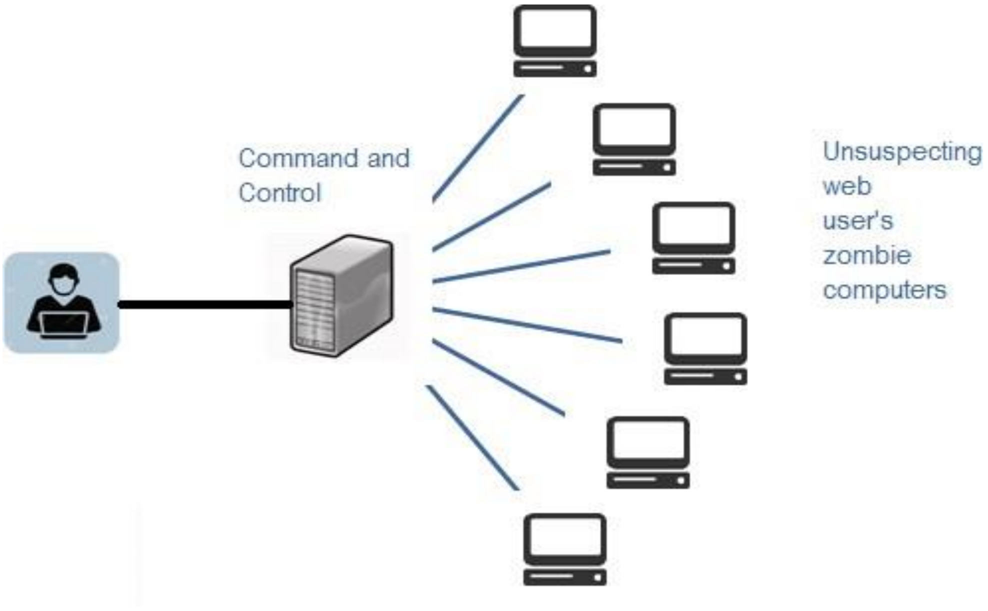
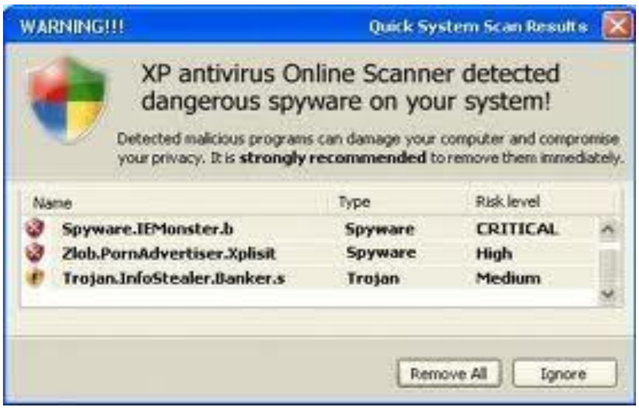


Figure 2: A typical botnet

1.3.7 Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user’s computer. As a remedial measure, the message suggests the used download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid. A sample message alert of a scareware is shown below in the below figure.



WARNING!!!

Quick System Scan Results

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

Figure Sample Warning Message of a Scareware

1.4 KINDS OF CYBER CRIME

Various types of cyber crimes are:

1.4.1 Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

1.4.2 Child Pornography

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

1.4.3 Forgery and Counterfeiting

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

1.4.4 Software Piracy and Crime

Software piracy is an illegal reproduction and distribution for personal use or business. Download of songs, downloading movies, etc.

1.4.5 Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

1.4.6 Phishing

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as ***Vishing*** (voice phishing). Another form of phishing is ***Smishing***, in which sms is used to lure customers.

1.4.7 Computer Vandalism

It is an act of physical destroying computing resources using physical force or malicious code.

1.4.8 Computer Hacking

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator‟s original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

The hackers may be classified as:

- **White Hat**: white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.
- **Black Hat**: in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions. They find the security loopholes the system, and keep the information themselves and exploit the system for personal or organizational benefits till organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- **Grey Hat**: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.

1.4.9 Creating and distributing viruses over internet

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

1.4.10 Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming. An email can be classified as spam, if it meets following criteria:

a. Mass mailing: - the email is not targeted to one particular person but to a large number of peoples.
b. Anonymity: - The real identify of the person not known
c. Unsolicited: - the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

1.4.11 Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.

1.4.12 Online Auction Fraud

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered once the payment is made.

1.4.13 Cyber Squatting

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

1.4.14 Logic Bombs

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition. If the conditions hold true in future, the malicious action begins and based on the action defined in the malicious code, they either destroy the information stored in the system or make system unusable.

1.4.15 Web Jacking

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India.

1.4.16 Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

1.4.17 Denial of Service (DoS) Attack

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

1.4.18 Salami Attack

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

1.4.19 Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report.

1.4.20 Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The next section discusses some of the popular techniques to counter the cyber attacks.

2.1 AUTHENTICATION

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like *One Time Password* (OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an *SMS* or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

2.2 ENCRYPTION

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption.

If the same key is used to lock and unlock the data, it is known as **symmetric key encryption**.

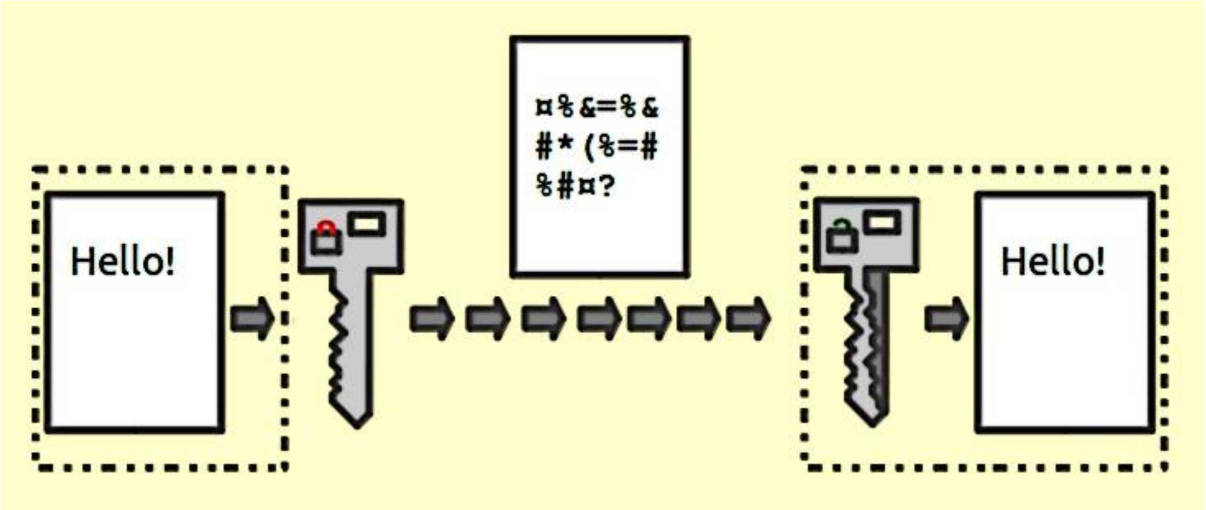


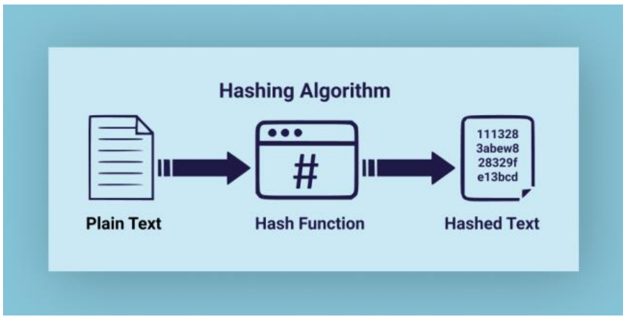
Figure 4: Encryption

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue.

To avoid the transfer of key a method called **asymmetric key encryption, also known as public key encryption**, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse's two keys, public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B"s public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be sent to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

Hashing is the process of converting data — text, numbers, files, or anything, really — into a fixed-length string of letters and numbers. Data is converted into these fixed-length strings, or hash values, by using a special algorithm called a hash function.

For example, a hash function that creates 32-character hash values will always turn text input into a unique 32-character code. Whether you want to generate a hash value for the word “Cybersecurity” or for the entire works of Shakespeare, the hash value will always be 32 characters long. A small change in the input value will result changes in the hash value. And the hash value is irreversible. Message Digest 5 (MD5), Secure Hash Algorithm (SHA) are the example of common Hashing algorithms.



2.3 DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key (which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is possess only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

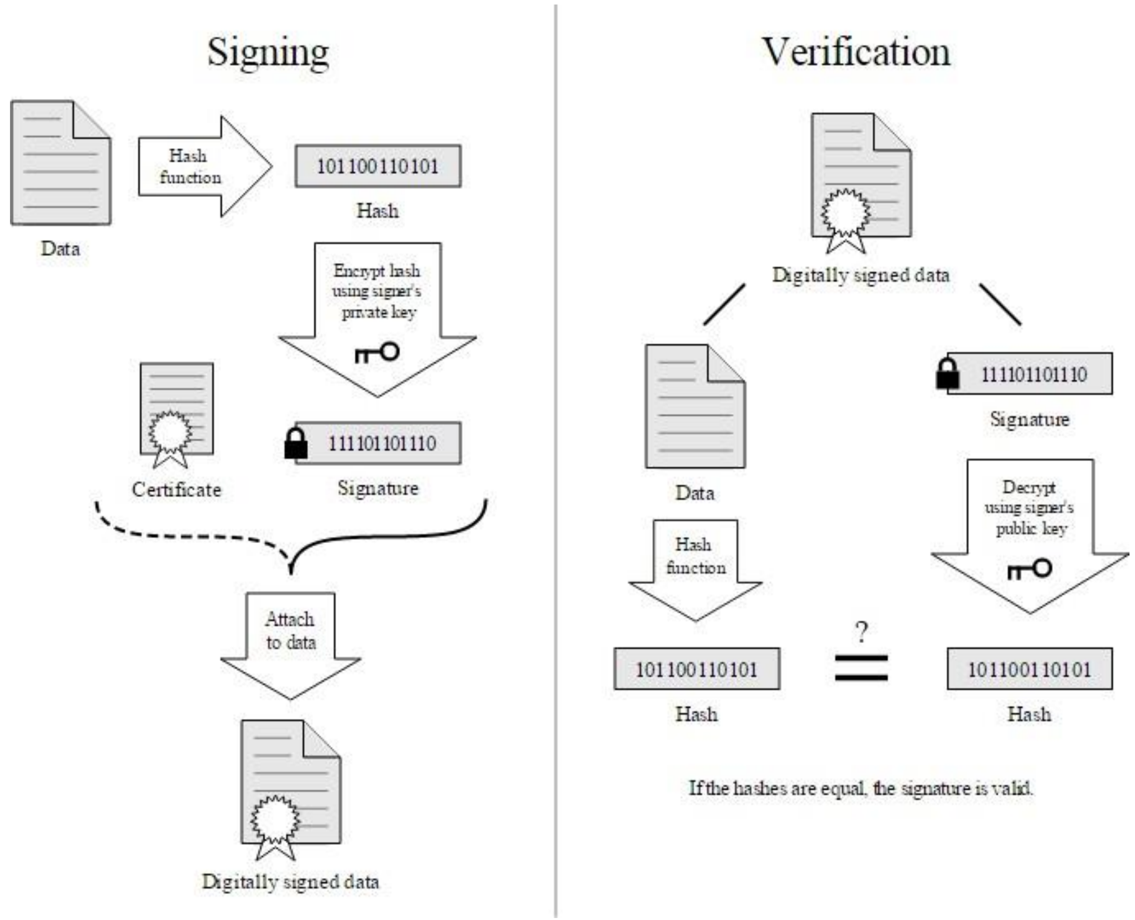


Figure 5: Digital signature

2.4 ANTIVIRUS

There are verities of malicious programs like virus, worms, trojan horse, etc that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

Figure 6: Different antivirus available on the market

2.5 FIREWALL

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.

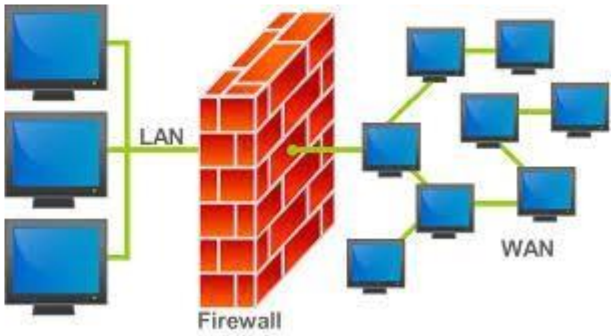


Figure 7: Firewall

There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.

The firewalls are an essential component of the organizations‟ network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch DOS attacks.

2.6 STEGANOGRAPHY

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.

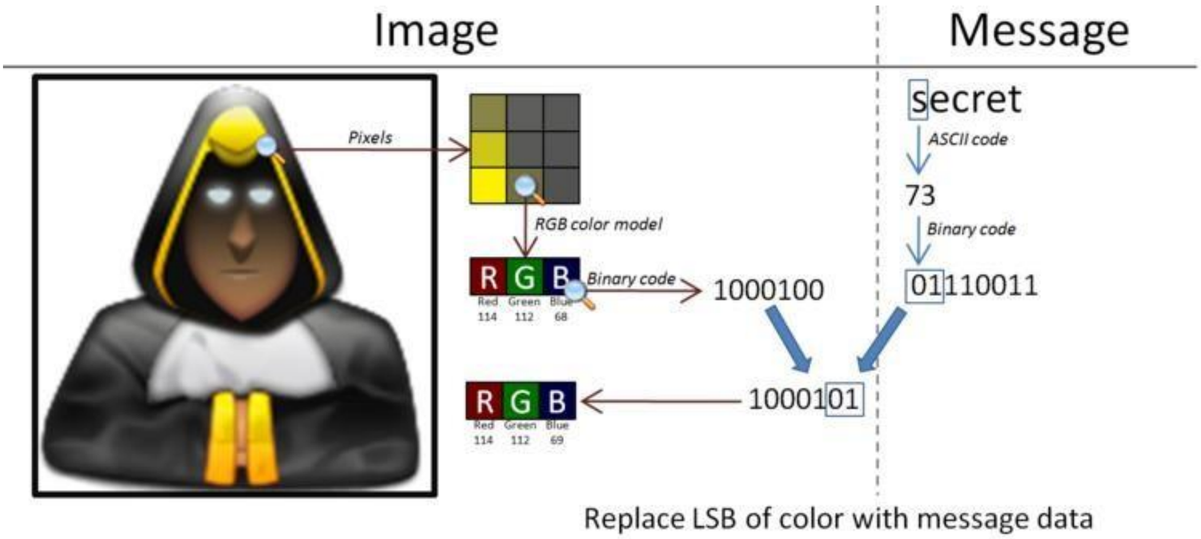


Figure 8: Steganography

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access.

Let us discuss how the data is secretly embedded inside the cover file (the medium like image, video, audio, etc. which is used for embed secret data) without being noticed. Let us take an example of an image file which is used as a cover medium. Each pixel of a high-resolution image is represented by 3 bytes (24 bits). If the 3 least significant bits of these 24 bits are altered and used for hiding the data, the resultant image, after embedded the data into it, will have un-noticeable change in the image quality and only a very experienced and trained eyes can detect this change. In this way, every pixel can be used to hide 3 bits of information.
Similarly, introducing a white noise in an audio file at regular or random interval can be used to hide data in an audio or video files. There are various free software available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

2.7 Digital Certificate?

2.8 TLS (Transport Layer Security)/ SSL (Secure Sockets Layer)?