International Journal of Recent Advances in Multidisciplinary Topics
Volume 4, Issue 4, April 2023
https://www.ijramt.com | ISSN (Online): 2582-7839


# Cyber Security and its Various Perspectives

Lakshit Chauhan*
*Student, Amity School of Engineering and Technology, Amity University, Noida, India*

***Abstract*: Cyber security is the techniques and technologies that are used to provide protection to computers, data and networks from unauthorized access. In this period of modernization, bundle of new advancement is coming but they also have comparably parallel dangers to economy and masses across the world therefore it's important for our young generation to get aware about the attacks and how they can be reduced in a much simpler and understandable manner. Attacks are executed via internet by attackers or cyber criminals and many major sectors are under risk of cyber-attacks including: financial sector, aviation sector, large corporations, government sector, etc. Where the primary issue is to provide secure and user-friendly services and there is panic to protect their data. The chief purpose of the research paper is to give the detailed review that how the various attacks are executed (including- Social Engineering Attack, DDoS Attack and MITM Attack), how various malwares work (including- Virus, worms and mass mailers, trojan horse, backdoors, Ransomware, Adware, Spyware, Spam, Rootkits) and how various cyber security techniques work (including- Antimalware Techniques, Cryptography, Encryption and Digital Signatures) to protect our systems from different attacks.**

***Keywords*: Cyber security, Malware, Cyber-attacks, Cyber security techniques.**

## 1. Introduction

Cyber security is an approach to protect the system, server and data by sharpening the security of huge foundations, businesses and organizations. Massive attacks are performed on an increasing rate every year to compromise any civilian or any targeted company due to their poor security system. Hence, users are more stressed over security of their information and services that they access over internet but users generally end up facing financial and data losses. Even more loss and breeches are waiting for us in near future which is a great worry. For a good Security knowing about Attacks is very important. There are numerous Sorts of Cyber Attacks in the market and the major attacks that are popular nowadays are described in the paper. Attacks also include installation of malwares too therefore; it's important to know how various malware works. Finally, the step comes where user needs to protect the system from malwares and attacks which is possible through various cyber security techniques. All these things are deeply explained in the paper.

### *A. Objective*

The objective of this research paper is to study about Cyber Security as a whole, that how the attacks are executed, how various malwares work and how the cyber-attacks can be reduced using cyber security techniques.

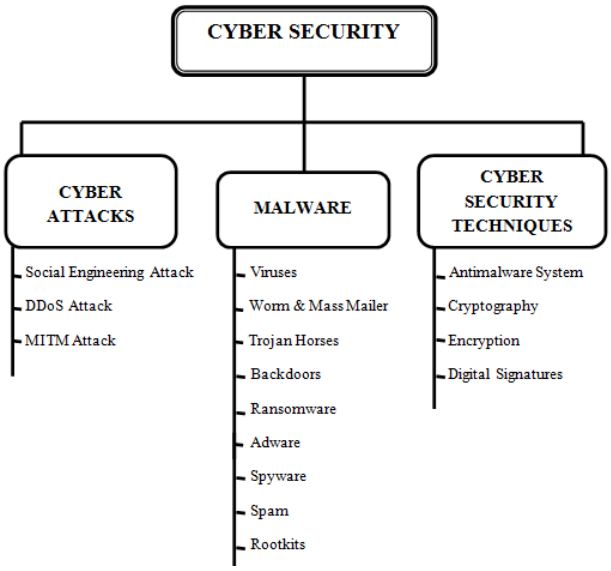


Fig. 1. Structure/Topics of research paper

## 2. Review

### *A. Cyber Attacks*

A cyber-attack attempts to disturb, disable, steal, gain unauthorized access, install malwares and destroy the network infrastructure etc. based on the attacker's motivation to attempt a particular attack. These attacks can be categorized on the three bases:

*Threat to Confidentiality:* In this category, there is threat to privacy means the private information can be known to the attacker who is attacking.

*Threat to Integrity:* In this category, there is the information can be tampered or edited by the attacker who is attacking.

*Threat to Availability:* In this category, there is threat to availability of any service means the service is not available to the user if it is attacked by the attacker.

### *B. Sorts of Cyber Attack*

Now based on these threats there are numerous Sorts of Cyber Attacks in the market and the major attacks that popular now a days are:

#### *1) Social Engineering Attack [1]*

Social Engineering Attack is used to perform Malicious

*Corresponding author: lakshit072001@gmail.com

Activities which can be done by Human Interactions. There are various social engineering attack techniques including:

*Baiting:* Baiting is done to spread malware and the Baits (like- ads) are made with a very authentic looks so that the people take baits out of their curiosity and install that into their computers which results in automatic malware installation on their systems. Baiting can be done through physical media where attackers leave baits in some areas (like- parking areas) of the targeted company which encourage people to install malware-infected applications into their systems. On the other hand, Baiting can also be done digitally where the bait redirect user to malware infected websites etc.

*Scareware:* In this, attacker gives fictitious threats to the people (like– Your computer is infected and you need to install this particular software) and people get into trap and install the prompted software which itself has malware and has no real benefit at all, by this their system gets infected by malware. Scareware is distributed via spam e-mails and by the popup banners which appear in the browser while web surfing.

*Pretexting:* Here, a false scenario is created by the attacker to collect the information of a person by showing him that the attacker is actually the person in power (like- HOD of a company where the victim works) and wants to confirm the victim's identity. By this technique the attacker can collect any sort of information of the victim. It can be done by IP Spoofing and SIM Card Cloning etc.

*Phishing:* Here, emails and text messages are sent to victim in order to generate sense of curiosity and urgency in victim. And then asks victim to disclose the sensitive details, clicking on link of malware infected websites and opening the attachments containing malware. For Example: A victim got mail by an online service which he accesses and that email alerts the victim of policy violation and asks him to change his password on his end which also contains a link of an illicit website where he needs to do the changes in his password and that website is nearly same in appearance to its original version. After the submission victim's information is collected by the attacker.

*Spear Phishing:* This is a more focused sort of the phishing where attacker choose particular individual or enterprise. In this the attacker alters message on the basis of victim's characteristics and employment position to execute attack in a hidden and undoubtful manner. This attack needs more efforts. For Example- the attacker creates a phishing scenario where he impersonates as company's IT Head and sends email to employees which is formulated and signed exactly as the original IT Head normally does. The message instructs the employees to edit their password and it supplies them with a link that takes them to a malicious webpage where their information is captured.

Social Engineering Attack can be prevented by not opening unknown emails or attachments, updating antivirus or antimalware software timely and beware of the attractive offers.

*2) DDoS Attack [2]*

Unlike other attacks, DDoS attack aims to make services unavailable to licit clients. It is executed with the help of huge number of different owner's system across the internet (BOTNETS) which are infected from malicious software and are in control of attacker. Here, the Attacker's Motivation is to get the denial of service of the targeted organization. Whereas, this attack can also be used by the attacker for Extortion as now the targeted organization is unable to provide services to its clients. DDoS Attacks can cause loss of revenues, information, trust and reputation of an organization.

*Types of DDoS Attack:*

Application Layer Attack (layer 7 attack): It aims to flood a server by sending a massive number of requests to use resource which demands in-depth handling and processing. It also includes the techniques of flooding like: HTTP flood etc. The size of this layer is measured in RPS (requests per second) and 50 to 100 RPS can easily disable medium sized websites.

Network Layer Attack (layer 3-4 attack): This attack aims to clog the "pipelines" connecting the network. It also includes the techniques of flooding like: UDP flood etc. DDoS attacks are due to huge traffic flow that can be measured in Gbps or PPS (packets per second). And 20 to 40 Gbps can easily damage most of the network infrastructures.

How DDoS attacks aim to deplete Network Resources and How we can reduce it?

Most important asset for any company is its Network and this attack can deplete the network which is a great panic for the organizations.

Now network resources can be classified into two categories:

*Network Capacity:* Network Capacity is comparably easy to deplete. DDoS attack is executed within few minutes which can bury majority of websites and networks. To avoid network pipe congestion a network demands for a notable network capacity, but it is comparably expensive strategy for standard business. So, DDoS protection services are better where the service providers increase network bandwidth (greater than the largest DDoS attack observed) so that there are no issues for sheer volume of the attack.

*Network Infrastructure:* Now the network capacity barrier is controlled but still there is lot of traffic to be handled and processed so the DDoS protection services, will provide routers, switches and other protection devices. Mostly headers of the packet are checked by the network devices and the full pay load is not inspected. The limiting factor is studied as packet rate not packet size. To provide protection, the PPS challenge is huge as it involves different sorts of protection techniques which demands for more processing power as compared to what is normally required to route or switch a packet.

*3) MITM (Man in the Middle) Attack [3]*

In this the attacker creates his position between the user and the application when the user is communicating with the application to imitate one of them and to show as if standard communication is going on. The aim of this attack is to steal the sensitive details such as passwords etc. Attacker usually targets the users of financial services for this attack like- users of e-commerce websites where logging in is required. Details collected by the attacker can be utilized for various motives like- password change, identity theft and illicit money transfer etc. It is also known as session hijacking as the attacker takeover

any session going between any application or server and a client.

It is performed in a certain matter which includes:

1) Client gets connected to any server.
2) Attacker's device will achieve control over client's device.
3) Client's device gets disconnected from the server by the attacker.
4) Attackers will replace his device IP address with client's IP address and client's sequence number will also be spoofed by the attacker.
5) Now the session continues between the server and attacker's device and the server believes that its communication is still going on with the genuine client.

MITM Attack Progression: It consists of 2 phases Interception and Decryption.

*Interception:* It can be performed easily by doing passive attack. Passive Attacks are performed in a way that the attacker will create a free malicious WIFI hotspot at public areas whose name corresponds to the location and is not password protected. So, now if anyone connects to that hotspot then the attacker will attain complete visibility to the online data exchange made by that person and if the attacker is having more active approach towards interception then he can launch some attacks including IP Spoofing, ARP Spoofing and DNS Spoofing etc.

*Decryption:* After interception, to get all the information of the victim a two-way SSL traffic is required to get decrypted to attain information from SSL without alerting the user or application which can be done by numerous ways like- HTTPS Spoofing etc.

MITM Attack can be prevented by avoiding the use of any public network while performing sensitive transactional activities, avoiding the use of WIFI which are not password protected and logging out from sensitive apps when not in use.

### C. MALWARE [4]

Malware is known as "poisonous programming.". It is designed to attain entry or perform any mischief with PC without the permission of the owner. Malware is a program which must be clicked or by a couple of procedures it gets executed before it can destroy the PC structure and spread to other systems. Malware generally spreads through emails, removable media or when a person downloads any infected software etc. It can allow the unauthorized access to System Resources, hence can cause data loss, financial loss, account theft, slows computer and internet speed.

### D. Sorts of Malware

There are distinctive sorts of malware which can incorporate different security hazard.

It is observed in Fig. 2 that the major portion of malware threat is due to Trojan horse followed by Viruses, Worms and others.

*Virus:* Virus needs a user to run the program to start working and it cannot copy themselves and cannot move through one device to other without a host to operate the program. Virus has to be allowed to execute the code and to write in the memory, that's why most of the virus join them through executable files (like-section of any licit program). This is also known as code injection.

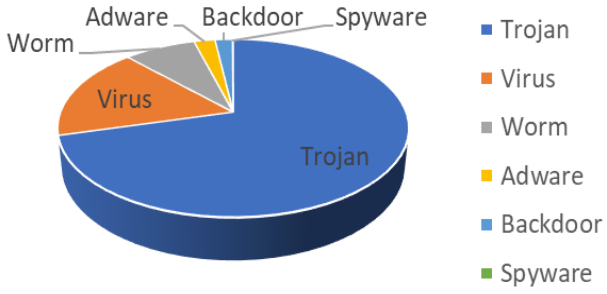


Fig. 2. Sorts of Malware Spread

*Worm:* It is the only computer malware program which can replicate itself to spread to other computers. It utilizes recursive method to copy themselves without host program. They are used to spread and gain control on more computers in short time but they can't attempt to perform changes in the system from which they travel through. Worms use the infected system as a host to infect other devices. Whereas, Mass Mailing is a technique in which large number of mails are send to victim to fill his email inbox and to crash it. It is mostly done when any important mail is there in the inbox and by doing this the inbox gets crashed or the important mail gets hide within that spam mails.

*Trojan Horses:* It's a most common type of malicious software which looks correct but actually carries concealed negative function that gets activated by starting the application. They require a user to run a program for execution that's why they persuade user to install it. Trojan horse can't be copied from one device to other themselves. However, they can cause same damage as normal virus does. It can also permit malware writer to control victim's system and to install more malwares.

*Backdoors:* Backdoor is a method of gaining access to a program, encryption, online service and computer system but in an undocumented way. It basically escapes standard authentication mechanism and is often known to programmer who created that program to troubleshoot or restore the password of the user if needed.

*Ransomware:* It threatens to publish victim's details and don't allow him to access data. Some advanced ransomware encrypts the files of victim by which the file becomes inaccessible and then the attacker demands money to decrypt, this is known as crypto viral and recovering file without decryption key is unmanageable process. Ransomware can be brought by Trojan Horses.

*Adware:* Adware shows advertisements to the users and persuade them to go to the websites by which attacker finds personal information of victim (like- Age, Job and Gender etc.) and attacker can sell those details to someone who require that and can earn money. Adware is comparatively easy to uninstall.

*Spyware:* A Spyware is a kind of adware but is more dangerous as it steals important information like- login

credentials etc. It is even harder to uninstall from the computer than adware. They do not even do anything to the victim's computer, regardless of abusing computers for business benefits.

*Spams:* Spam is an undesirable email that a user doesn't ask for. One individual's spam might be useful for the outline development or whatever else for any attacker to attack. It is a standard approach to manage and regulate the spread of noxious programming like- Trojans, Viruses and so forth which can infect the user's system.

*Rootkits:* It is collection of malicious software which is made to gain access to computer or certain programs as an unauthorized user. "Root" means targeted admin account and "kit" means software components that implement tools. Rootkits do admin modifications in which the attacker change the security settings and the user account permissions (Usually controlled by computer admin). Rootkits cannot spread by themselves and attacker will do the modifications in such a way to get full access to cause damage by which it is difficult to detect it.

### *E. Cyber Security Techniques*

Cyber Security techniques are required to protect our systems, server, data and network from various cyber-attacks and malwares in order to provide Confidentiality, Integrity, Availability and Authentication to the system.

#### *1) Anti-Malware System*

Antimalware framework is utilized to see PC pollutions, Trojan steeds and to expel them from the PC structure. Antimalware System Technique includes:

a) *Anti-Virus:* It is used to shield the PC framework against dangerous programs. Antivirus programming needs to keep running in foundation tirelessly, and it must be provided with the target that it can see new kind of destructive programming. It's a sort of structure that is proposed to secure and see and expel undesirable spyware programs from the system if showed.

b) *Anti-Spam Programs:* It tries to see the purposeless or dangerous messages present as an email.

c) *Firewall:* Its job is to monitor and control the network traffic coming inside or going outside on the basis of some security rules. Moreover, firewall creates a wall between trusted network and the untrusted network by stopping all unauthorised IP addresses and Port Numbers. E.g.: Network based and Host based Firewalls

#### *2) Cryptography [5]*

Cryptography is an effective and popular data security technique where the word "cryp" means hidden and "graphy" means writing. In Cryptography process, the Plaintext or the non-encrypted data which is in the readable format is converted into the Ciphertext or the encrypted data which is now in the Non readable format with the help of Encryption. Ciphertext can be then converted back again into the Plaintext with the help of Decryption. Individuals who practice in this field are called Cryptographers.

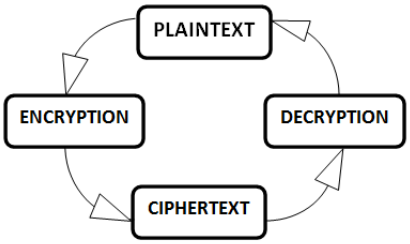


Fig. 3. Cryptography process

Cryptography applies various algorithms to shuffle the bits which represents the data in such a way that only the authorized user can unshuffle that to obtain original data. Cryptography algorithms use unique and clever mathematics to achieve effective shuffling. Most common Cryptographic Standards are open and these Open Standards (where cryptography algorithms are known and published) helps to ensure that the cryptography is secure or not. But nowadays, clever mathematics makes it really impractical to decode the shuffled bits easily. Cryptography includes study of encryption and decryption whereas encryption requires study of encoding. Cryptography applies checks to empower the bits that address data with a total concentration on those selected customers who can unshuffle them to get the key data. Encryption is one of the components of Cryptography enables to store sensitive information or transmit it across any networks (like Internet) and the information cannot be read by anyone except the authorized receiver. It plays a major role to many models of robotized security.

#### *3) Encryption [6]*

Encryption encodes data into ciphertext and it cannot be decrypted back without applying of a specific key which can unlock it. In encryption, a person needs to solve complex mathematical related complications which requires massive amount of time and computing resources.

Encryption is of two sorts: Symmetric and Asymmetric Encryption

In Symmetric Encryption, keys which are utilized in data encryption and decryption are same, and so the level of security is also similar. There are potential security risks in distribution of keys.


Fig. 4. Symmetric encryption

In Asymmetric Encryption, public key is utilized for data encoding and a private key is utilized for data decoding. Most of the security protocols use Asymmetric Encryption for keys distribution.

There is a drawback in Symmetric Encryption, that is potential loss of private key as if the private key is lost, system is rendered void. To mitigate that, public key infrastructure is used which is a combination of both private and public key, so loss of private key doesn't affect the system.

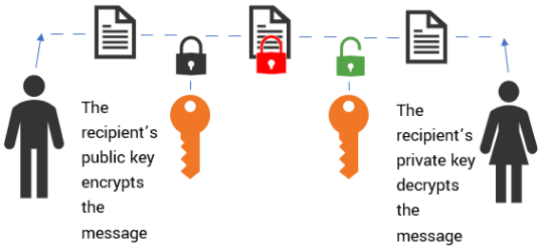


Fig. 5. Asymmetric encryption

*Public Key:* It is utilized for data encryption. They are produced by which anyone can be able to send data to specific receiver to access a message securely.

*Private Key:* It is utilized for data decryption which are encoded with the public key which gets match to the private key and private keys are created to be kept secret.

The nature of relationship between private and public key is mathematical and related to cryptographic algorithm. A conspicuous Internet security tradition that uses asymmetric encryption is the SSL (Secure Sockets Layer). SSL is usually utilized by projects and Internet servers while transferring private information. While realizing SSL traditions, a program will exhibit a URL with "https".

*Cyber Security Tips for Encryption:* As, Remote controlled devices are easy for to exchange off by attackers therefore, tricky, important and sensitive information should be encoded. One must also retain his private keys arranged and guaranteed by password. Advancement encourages extended use of affirmation in perspective of biometrics, for instance, extraordinary check, retina and face looks at, and what's more voice conspicuous evidence.

*4) Digital Signatures [7]*

Anyone can make a private/public key pair. It's not a difficult task, given today's toolkits. So, if I am giving my public key to anyone, along with the encrypted data without digital signatures it is not completely secure because to really trust that I am who I say I am is not possible and we need someone to sign off to make sure of his identity so, there comes the role of Digital Signatures. A propelled check is used to attest the validness of the sender of a message. It will in like manner affirm that the information has not changed. In case anything in the report is changed after the propelled check has been joined, the stamp twists up observably invalid. Therefore, it can be used with or without encryption.

"Encrypted data" and "Signature" aren't the same thing. Anyone can provide a signature on a plaintext message so that, if some other person has the public key, he can verify that it came from that person and there's no requirement for the data encryption. In Digital Signature Technique, private key is known just by the proprietor, it is used to pass on the induced stamp for a specific record and the public/open key is used to check the realness of the stamp while in Encryption, originators of encoded messages use an open key to send to recipients who use private keys to unscramble the message or information. Nowadays, Organization required the proper mechanism to monitor the fairness and authentication of documentation for a legitimate perspective.

An average robotized check plot:

1) A check estimation which, taken as data a message m and a private key SK produces a stamp σ.
2) An affirmation count which, taken as data the message m, open key PK and a check σ, sees or rejects the stamp.

*Digital Signature Process:*

A Digital stamp is a bound hash, of the main data, that has been mixed with the guarantor's private key. A robotized check process is made by the running with strides. The sender figures the hash for the data he needs to sign. The hash work is passed on limiting the likelihood to get a comparative estimation of the strategy from different messages and is in like way "one way" work.

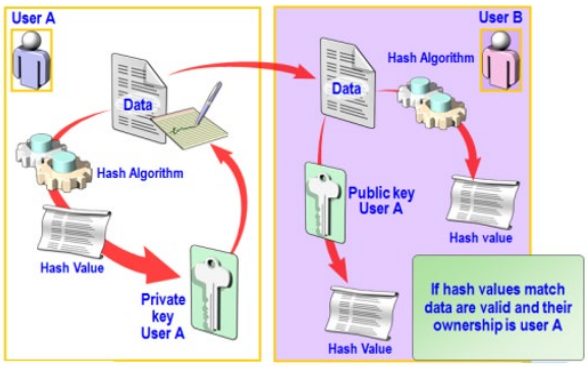


Fig. 6. Digital signature process

For a check, suppose a data is sent from one person to other then using digital signature a hash value is generated and then that hash is encrypted using primary key by the sender. After receiving the data by the receiver, it will check the hash value generated by hash algorithm which was actual value and the other hash value that is decrypted using public key and if both the hash is same then it confirms the security of the data that nothing is changed in the data received. Digital Signatures are a kind of double check using encryption.

By this technique, the receivers can confirm the identity of sender (authenticity), the sender is unable to deny that he showed something (non-denial) and the receiver can't plan or change a record set apart by someone else (respectability)

## *F. Result and Discussion*

As cyber-attacks are drastically increasing every year so it's important to get aware about the attacks and how they can be reduced. Therefore, the paper provides clear explanation about how these cyber-attacks are executed by describing different sorts of cyber-attacks practiced to gain benefits. Basically, these attacks are completely based on threats to CIA. The paper also explains that how various malwares work and how cyber-

attacks can be reduced by describing various cyber security techniques to protect our system from various malwares and cyber-attacks.

## 3. Conclusion

If the people and organizations understand Cyber Security and implement the appropriate cyber security technique then from the smallest attack to the bigger attack, rate of attacks can be decreased to a large extent because after all the research and deep study the conclusion is that Cyber Security is the only way which can reduce the rate of Cyber Attacks and make our systems, servers, data and network safe and secure. Nowadays in government sector also public information like- identity card, passport are digital records and can be misused and most developed countries now agree that cyber-attacks are the top threats to the security of country and there is a need to give edge security and hence there is a huge scope for cyber security.

## References

[1] Social Engineering [HTML document], https://www.imperva.com
[2] DDoS Attacks [HTML document], https://www.imperva.com
[3] Man in the middle (MITM) attack [HTML document], https://www.imperva.com
[4] Malware Types [HTML document]. https://www.imperva.com
[5] Cryptography [HTML document], https://www.synopsys.com
[6] Encryption [HTML document], https://medium.com/searchencrypt
[7] Digital Signatures, https://i2.wp.com/securityaffairs.co/wordpress/wp-content/uploads/2012/05/Digital_Signature_Sign_verify.png