International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

CYBER SECURITY

Yasser Khan (Assistant Professor) , Shashwat Srivastava

MASTER OF BUSINESS ADMINISTRATION

School of Business

Galgotias University

ABSTRACT

Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology (OT) security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term “cybersecurity” as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term “cybersecurity” to designate only security practices related to the defensive actions involving or relying upon information technology and/or OT environments and systems. Within this paper, we are aiming to explain “cybersecurity” and describe the relationships among cybersecurity, information security, OT security, IT security, and other related disciplines and practices, e.g. cyber defence, related to their implementation aligned with the planned or existing cybersecurity strategy at the national level. In the case study given example of The National Cybersecurity Strategy of the Republic of Croatia and Action plan is presented and elaborated. The Strategy's primary objective is to recognize organizational problems in its implementation and broaden the understanding of the importance of this issue in the society.

INTRODUCTION

Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and focus person has a potential target. However, such discussion on cyber security has important implication as it focuses on the ethical part of the society as a whole. To address the issue of cyber security, various frameworks and models have been developed. It also introduces the concepts of cyber security in terms of its framework, workforces and information related to protecting personal information in the computer. This paper reviews these models along with their limitations and review the past techniques used to mitigate these threats. Furthermore, the report also provides recommendations for future research.

Internet is among the most important inventions of the 21st century, which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don‟t even require a computer for using internet. Now we have internet-enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective.

1.2 INTRODUCTION TO CYBER CRIME

The internet was born around 1960‟s where its access was limited to few scientist, researchers and the defence only. Internet user base have evolved expontinanlty. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980‟s, the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Until then the effect was not so widespread because internet was only confined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle. The GUIs were written so well that the user do not have to bother how the internet was functioning. They have to simply make few click over the hyperlinks or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or weather the data can accessed by another person who is connected to the internet or weather the data packet sent over the internet can be spoofed and tempered. The focus of the computer crime shifted from merely damaging the computer,

destroying, or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every second around 25 computer became victim to cyber-attack and around 800 million individuals are affected by it until 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around $160 million are lost per year due to cybercrime. This figure is very conservative, as most of the cases are never reported. According to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is a third largest number do Internet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers (ISPs).

Before discussing the matter further, let us know what the cyber-crime is?

The term cybercrime is used to describe a 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. The people of destructive and criminal mind-set for either revenge, greed or adventure often commit it.

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:

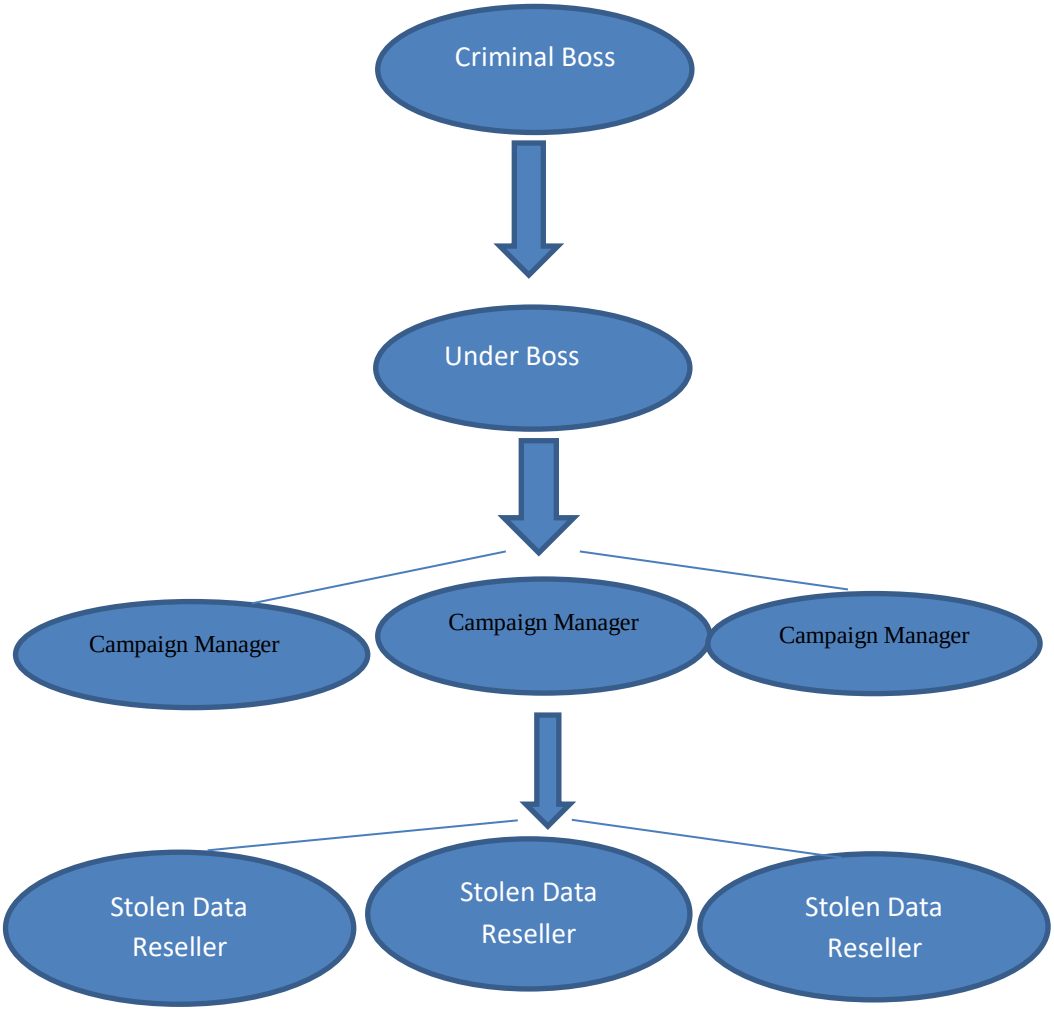
- Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber-attack, as he is well aware of the policies, processes, IT architecture and wellness of the security system. Moreover, the attacker have an access to the network. Therefore, it is comparatively easy for an 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 variability window for the attacker. The insider attack could be prevented by planning and installing an internal intrusion detection system (IDS) in the organization.
- External Attack: When an insider or an external entity to the organization hires the attacker, 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 experiment network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analysing these firewall logs. In addition, 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. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when an internal employee performed a structured attack. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

- Unstructured attacks: armatures who do not have any predefined motives to perform the cyber-attack generally perform these attacks. Usually these armatures try to test a tool readily available over the internet on the network of a random company. Structure Attack: highly skilled and experienced people perform these types of attacks 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 attackers 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.

Cyber-crimes have turned out to be a low-investment, low-risk business with huge returns. Now days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are into online drugs trading.

Figure 1: Hierarchical Organisational Structure



The role of all the people in the hierarchy remain changing and it is based on the opportunity. If a hacker, who have hacked sensitive data from an organization may use it for financially exploiting the organisation himself. In case, the hacker himself have the technical expertise for it, he will do it himself; otherwise, he may find a buyer who is interested in that data and have the technical expertise.

There are some cyber criminal's offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensitive data, or create massive denial-of –service attack on their competitors. Based on the demand of the customer the hackers write malware, virus, etc. to suit their requirements. An organization effected by a cyber-attack, not only faces financial loss, but its reputation is also adversely affected, and the competitor organization will defiantly benefited by it.

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 pride if someone hack the highly secured networks like defence 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. It is much easier to get away with criminal activity in a cyber-world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.
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.

1.4 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 behaviour 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 related to IPRs Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are 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 Smiting, 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.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

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

Many genuine websites offer 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 that 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 holds 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, economic 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 in 2014.

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 Attack

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

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, his actual salary in the report replaces the total salary.

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.

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access, which is present in a centralized, sever. Alternatively, an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of

giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization. Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk. Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defence agencies, financial institutions, planning commissions, etc. a hybrid authentication system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use VPN (Virtual Private Network), which is one of the method to provide secure access via hybrid security authentication to the company network over internet.

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, 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 encryptio

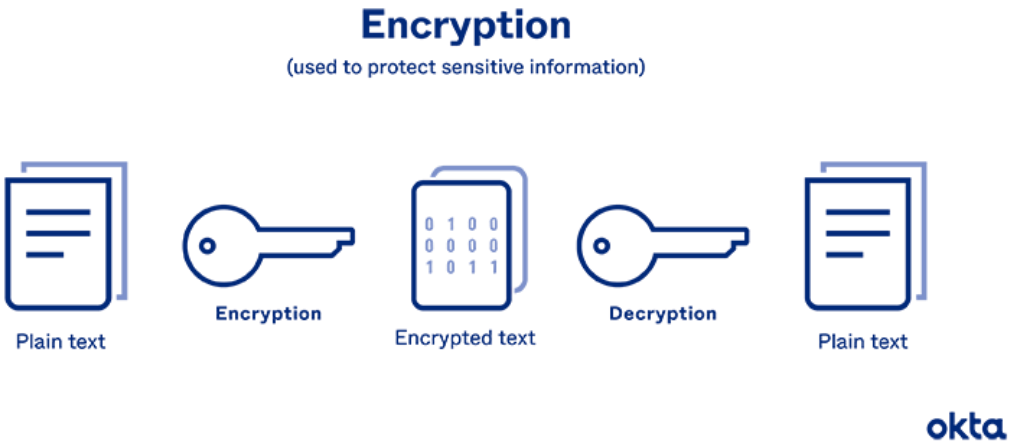


Figure 2: Encryption

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 viz. public key and private key. As the name suggest, everyone knows the public key of every user 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 send 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.

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, the receiver easily detects it, 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.

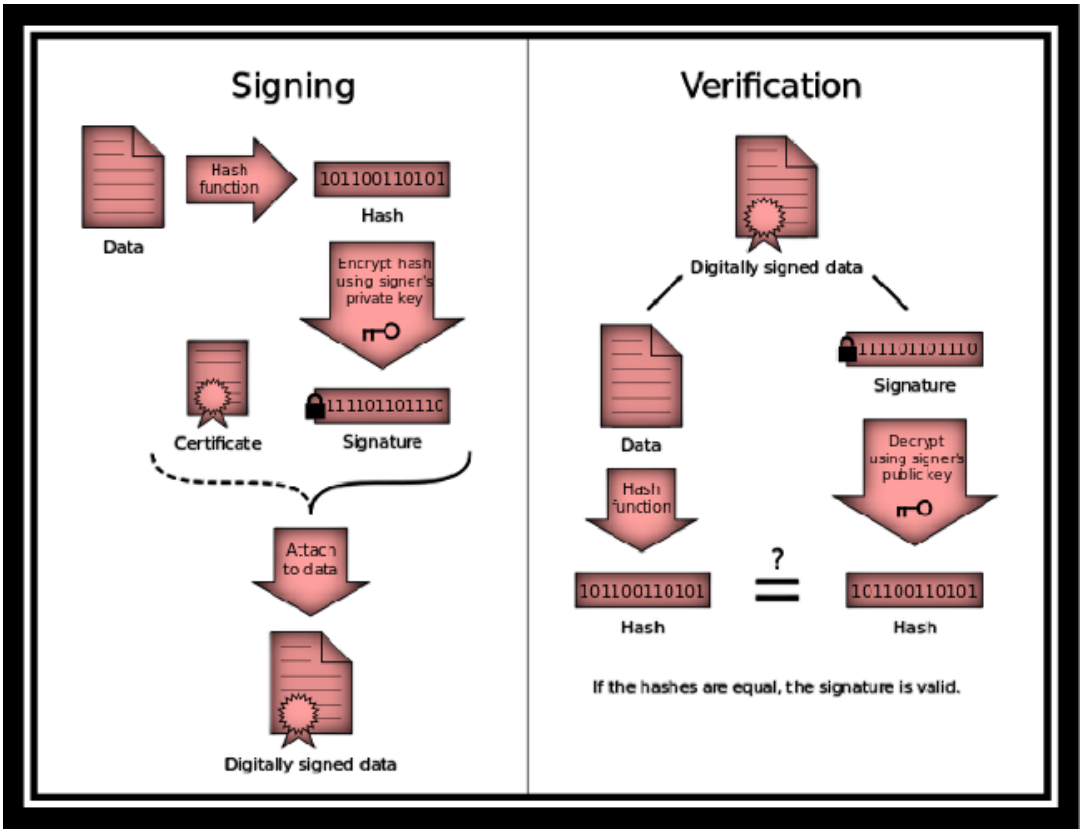


Figure 3: Digital Signature

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 4: Different Antivirus available in 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.

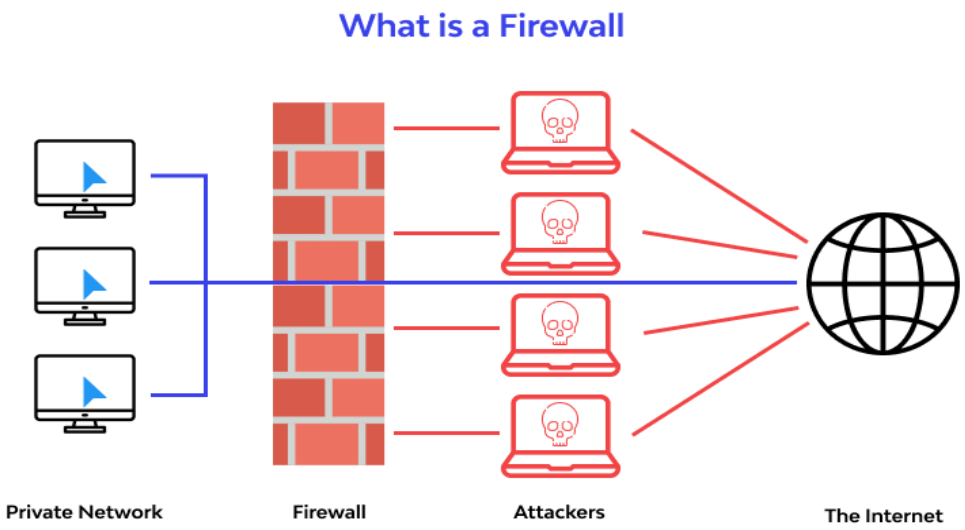


Figure 5: Firewall

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. In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system.

The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow "rules" and "policies" and based on these defined rules the firewalls can follow the following filtering mechanisms.

- Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- Stateful Inspection: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

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.

There are many applications of steganography, which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc.

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 three 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 unnoticeable 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 audio or video files. There are various free soft wares available for Steganography. Some of the popular ones are QuickStego, Xiao, Tucows, OpenStego, etc.

INVESTIGATING CYBER CRIMES: INTRODUCTION TO CYBER FORENSIC

In the preceding chapters, we have discussed the prevention techniques for cyber-attack. What if one have encounter cyber-attack? What Next? The next step is to report the cyber-crime. However, if a person is exposed to cyber forensic principles, the chances that the person accidently destroy the vital cyber evidences are minimized.

3.1 COMPUTER FORENSICS

Cyber forensic is a branch of science which deals with tools and techniques for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a practice of preserving, extracting, analysing and documenting evidence from digital devices such as computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in legal/administrative matters.

The computer forensic plays a vital role in an organization as the dependency on computing devices and internet is increasing day-by-day. According to a survey conducted by University of California7, 93% of all the information generated during 1999 was generated in digital form, on computers; only 7% of the remaining information was generated using other sources like paper etc. It not always easy to collect evidences, as the data may be tempered, deleted, hidden or encrypted. Digital forensic investigation is a highly skilled task, which needs the expose of various tools, techniques and guidelines for finding and recovering the digital evidences from the crime scene or the digital equipment used in the crime. With digital equipment like smartphone, tablets, palmtops, smart TV, etc. having increasing processing capabilities and computation speed, the possibility of use of these devices in cyber-crime cannot be ruled out. A forensic investigator must not only have deep understanding of the working of these devices and hands-on exposure to the tools for accurate data retrieval so that the value and integrity of the data is preserved.

A computer can be used intentionally or unintentionally to cyber-crime. The intentional use is to use your computer to send hate mails or installing cracked version of an otherwise licenced software into your computer. Unintentional use is the computer you are using contains virus and it is spread into the network and outside the network causing major loss to someone in financial terms. Similarly, a computer can be directly used to commit a digital crime. For example, your computer is used to access the sensitive and classified data and the data is sent someone inside/outside the network who can use this data for him own benefit. The indirect use of computer is when while downloading a crack of a software, a Trojan horse is stored in the computer, while creates a backdoor in the network to facilitate hacker. Now the hacker logs into your computer and use it for committing cyber-crime. An experienced computer forensic investigator plays a crucial role in distinguishing direct and indirect attack. Computer forensic experts are also useful for recovery of accidental data loss, to detect industrial espionage, counterfeiting, etc.

In large organization, as soon as a cyber-crime is detected by the incident handling team, which is responsible for monitoring and detection of security event on a computer or computer network, initial incident management processes are followed8. This is an in-house process. It follows following steps:

1. Preparation: The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.
2. Identification: based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.
3. Containment: based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step.
4. Eradication: In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed.
5. Recovery: it is the process of returning to the normal operational state after eradication of the problem.
6. Lesson Learned: if a new type of incident is encounter, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is mostly performed by third party companies. The computer forensic investigation involves following steps:

1. Identify incident and evidence: this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.
2. Collect and preserve evidence: Various tools like Helix, Win Hex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5 (message digest) hash of the backup is