Firewall

Definition:

Firewall is a network security device that observes and filters incoming and outgoing network traffic, adhering to the security policies defined by an organization. Essentially, it acts as a protective wall between a private internal network and the public Internet.

Fencing your property protects your house and keeps trespassers at bay; similarly, firewalls are used to secure a computer network. Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.

Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Uses of Firewall

- The most important function of a firewall is that it creates a border between an external network and the guarded network where the firewall inspects all packets (pieces of data for internet transfer) entering and leaving the guarded network. Once the inspection is completed, a firewall can differentiate between benign and malicious packets with the help of a set of pre-configured rules.

- The firewall abides such packets, whether they come in a rule set or not, so that they should not enter into the guarded network.

- This packet form information includes the information source, its destination, and the content. These might differ at every level of the network, and so do the rule sets. Firewalls read these packets and reform them concerning rules to tell the protocol where to send them.

What can do Firewall:

A firewall is a critical part of network security that acts as a barrier between a trusted internal network and untrusted external networks like the internet. Here are some things a firewall can do:

- **Packet Filtering:** It examines packets of data coming into or leaving the network and determines whether to block or allow them based on predetermined security rules.

- **Access Control:** It can control who has access to the network by setting rules and permissions for inbound and outbound traffic.

- **Stateful Inspection:** A more advanced firewall can track the state of active connections and make decisions based on the context of the traffic flow.

- **Proxying and Network Address Translation (NAT):** It can act as an intermediary between a user and the internet, hiding the actual network addresses of the devices behind it.

- **Logging and Monitoring:** Firewalls often keep logs of network traffic, which can be monitored for security incidents, anomalies, or patterns that might indicate a security threat.

Virus

Definition:

Computer viruses are unwanted software programs or pieces of code that interfere with the functioning of the computer. They spread through contaminated files, data, and insecure networks. Once it enters your system, it can replicate to produce copies of itself to spread from one program to another program and from one infected computer to another computer. So, we can say that it is a self-replicating computer program that interferes with the functioning of the computer by infecting files, data, programs, etc.

Uses of Virus:

Computer viruses, despite being malicious, have had various uses, not all of which are ethical or legal. Here are some contexts where computer viruses have been used:

- **Malicious Intent:** The primary use of computer viruses is for malicious activities. They're designed to infect systems, corrupt data, steal information, or disrupt normal computer operations. These can range from ransomware that encrypts files for extortion to spyware that steals sensitive information.

- **Cyber Espionage:** Viruses have been employed to spy on individuals, organizations, or governments, aiming to steal confidential information, intellectual property, or state secrets.

- **Botnets:** Viruses can be used to create botnets—networks of infected computers controlled by a single entity. These botnets can carry out distributed denial-of-service (DDoS) attacks, sending massive amounts of traffic to overwhelm servers or networks.

- **Testing and Research:** Ethical hackers and cybersecurity researchers may use viruses in controlled environments to study their behavior, understand vulnerabilities, and develop countermeasures to protect against them.

- **Proof of Concept:** Sometimes, security experts or researchers create viruses to demonstrate vulnerabilities in software or systems to highlight potential risks and encourage better security practices.

- **Government and Military Use:** Some governments may develop viruses for cyber warfare, either for offensive purposes to disrupt adversaries' systems or for defensive measures to protect their own networks.

Example:

- **Melissa:** Melissa was an email virus that spread through Microsoft Word documents attached to infected emails. Once opened, it would infect the user's system and automatically send infected documents to the first 50 contacts in the victim's email address book.

- **WannaCry:** This ransomware virus spread in 2017, exploiting a vulnerability in Windows systems. It encrypted files on infected computers and demanded a ransom in Bitcoin to unlock them. It affected numerous organizations worldwide, including hospitals and businesses.

- **Code Red:** This worm targeted computers running Microsoft IIS web server software. It would deface websites, spread itself to other vulnerable servers, and launch DDoS attacks against certain web servers.

- **Stuxnet:** Stuxnet was a highly sophisticated computer worm discovered in 2010. It specifically targeted supervisory control and data acquisition (SCADA) systems used to control and monitor industrial processes. It was designed to target Iran's nuclear program.

Spyware

Definition:

Spyware is a breach of cyber security as they usually get into the laptop/ computer system when a user unintentionally clicks on a random unknown link or opens an unknown attachment, which downloads the spyware alongside the attachment. It is a best practice to be cautious of the sites that are used for downloading content on the system. Spyware is a type of software that unethically without proper permissions or authorization steals a user's personal or business information and sends it to a third party. Spyware may get into a computer or laptop as a hidden component through free or shared wares.

Uses of Spyware:

Spyware is a type of malicious software designed to gather information about a person or organization without their knowledge. While its primary use is malicious, it has been utilized in various ways:

- **Information Theft:** Spyware can stealthily collect sensitive information like login credentials, credit card details, browsing habits, and personal data. This stolen information might be used for identity theft, financial fraud, or sold on the dark web.

- **Targeted Advertising:** Some less harmful spyware tracks browsing habits to create targeted advertisements. While this might not directly harm systems, it invades privacy by monitoring and utilizing personal information for advertising purposes without consent.

- **Espionage and Surveillance:** Governments, intelligence agencies, or malicious entities might deploy spyware to monitor individuals, organizations, or governments, aiming to gather sensitive information, state secrets, or intellectual property.

- **Parental Control and Employee Monitoring:** In certain legal and controlled contexts, spyware-like software might be used by parents to monitor their children's online activities or by employers to track employees' computer usage for security and productivity purposes.

Example:

- **ZeuS/Zbot:** This spyware targeted Windows-based systems and was notorious for stealing sensitive information, including banking credentials and personal data. It operated by logging keystrokes, capturing screenshots, and accessing personal information stored on the infected computer.

- **FinFisher/FinSpy:** Developed by a company called Gamma Group, FinFisher was marketed as a tool for law enforcement and intelligence agencies. However, it was used for surveillance purposes and could take screenshots, record keystrokes, and access files on infected computers.

- **Pegasus:** Developed by the NSO Group, Pegasus is sophisticated spyware capable of infecting both iOS and Android devices. It can remotely take control of a device, access messages, calls, and even activate the camera and microphone for surveillance purposes.

- **Superfish:** While not as malicious as some other spyware, Superfish was pre-installed on some Lenovo laptops. It injected third-party ads into web browsers by intercepting internet traffic, potentially compromising user privacy and security.

Malware

Definition:

Malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users. Malware can take many forms. It’s important for individuals and organizations to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

Uses of Malware:

- **Financial Gain:** Malware creators often aim to make money through various means:

- **Ransomware:** Encrypts files or locks users out of their systems until a ransom is paid.
- **Banking Trojans:** Steals banking credentials or conducts unauthorized transactions.
- **Adware and Click Fraud:** Generates revenue through intrusive ads or fake clicks on advertisements.
- **Data Theft:** Malware can be used to steal sensitive information like personal data, login credentials, intellectual property, or financial information. Stolen data might be sold on the dark web or used for identity theft and fraud.

- **Espionage:** Nation-states or corporate entities might use malware for espionage purposes, aiming to gather intelligence, monitor communications, or gain access to sensitive government or corporate information.

- **Disruption and Sabotage:** Malware can be used to disrupt systems, networks, or critical infrastructure, causing chaos, financial damage, or even endangering lives in extreme cases.

- **Botnets and DDoS Attacks:** Malware can create botnets—networks of infected devices controlled by a single entity. These botnets might be used for distributed denial-of-service (DDoS) attacks, overwhelming servers or networks with massive amounts of traffic.

- **Testing and Research:** Ethical hackers and cybersecurity professionals might use controlled malware samples to test network defenses, identify vulnerabilities, and develop countermeasures.

Example:

- **WannaCry:** This ransomware made headlines in 2017 by exploiting a vulnerability in Microsoft's Windows operating systems. It encrypted files on infected computers and demanded ransom payments in Bitcoin to unlock them. It spread rapidly across networks, affecting numerous organizations worldwide.

- **Emotet:** Initially a banking trojan, Emotet evolved into a sophisticated malware delivery service. It propagated through phishing emails, stealing sensitive information and distributing other malware, such as ransomware or other banking trojans.

- **Mirai:** Mirai targeted Internet of Things (IoT) devices, infecting them and turning them into a botnet used for launching massive distributed denial-of-service (DDoS) attacks. It caused widespread internet disruptions by flooding targeted servers with traffic.

Worm

Definition:

Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread. They are standalone computer malware that doesn't even require human support to execute. Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

Uses of Worm:

- **Research and Testing:** In controlled and ethical environments, worms can be used for research and testing cybersecurity defenses. Security experts might create worms to assess vulnerabilities, study propagation methods, and develop countermeasures against them.

- **Network Maintenance:** In certain cases, benign worms are used for network maintenance or updates, where they're programmed to distribute necessary patches or updates across a network efficiently.

- **Information Sharing:** Some non-malicious worms are designed for sharing information or distributing software updates across a network of computers, facilitating information exchange in a controlled manner.

- **Educational Purposes:** Worms can be used in educational settings to demonstrate how malware spreads and the importance of cybersecurity practices to prevent infections.

Example:

- **Conficker:** Conficker, also known as Downadup, was a highly sophisticated worm that targeted Windows operating systems. It spread rapidly by exploiting vulnerabilities in Windows, infecting millions of computers worldwide. It could disable security services, steal sensitive information, and create botnets for various malicious activities.

- **SQL Slammer:** Also known as the Sapphire worm, SQL Slammer exploited a vulnerability in Microsoft SQL Server and Desktop Engine. It propagated rapidly by sending a small packet of data to random IP addresses, causing widespread internet slowdowns and disruptions in 2003.

- **Morris Worm:** The Morris Worm, created by Robert Tappan Morris in 1988, was one of the earliest and most famous worms. It exploited vulnerabilities in Unix systems, spreading across the early internet and causing significant disruptions. Its intent was not malicious, but due to a flaw, it ended up infecting systems multiple times, causing congestion and slowdowns.

- **Code Red:** Code Red was a worm that exploited vulnerabilities in Microsoft Internet Information Services (IIS) web servers. It spread by generating random IP addresses and launching DDoS attacks against specific web servers, causing disruptions and defacing websites.

Trojan Horse

Definition:

The name of the Trojan Horse is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more. Now like many viruses or worms, Trojan Horse does not have the ability to replicate itself.

Uses of Trojan Horse:

- **Data Theft:** Trojans can steal sensitive information like login credentials, financial data, personal information, or intellectual property from infected devices. They might use keylogging, screen capturing, or other techniques to gather this information.

- **Backdoor Access:** Some Trojans create a "backdoor" on infected systems, allowing attackers to gain unauthorized access or control over the compromised device. This access can be used for further attacks, data theft, or espionage.

- **Botnet Creation:** Trojans can turn infected devices into bots, forming a network of compromised computers (botnet). These botnets can be remotely controlled to carry out various tasks, like launching DDoS attacks or distributing spam emails.

- **Ransomware:** Certain Trojans act as a delivery mechanism for ransomware. Once they infect a system, they can download and install ransomware that encrypts files, demanding a ransom for decryption.

- **Spyware and Surveillance:** Trojans might be used for covert surveillance, spying on users by activating webcams, microphones, or collecting sensitive information without the victim's knowledge.

Example:

- **Zeus/Zbot:** Zeus is a well-known Trojan that targeted Windows-based systems, primarily aimed at stealing sensitive information, especially banking credentials. It was highly effective in creating botnets and was often used for financial fraud.

- **SpyEye:** Similar to Zeus, SpyEye was a banking Trojan used to steal financial information and banking credentials. It had capabilities for keylogging, form grabbing, and manipulating online banking sessions to siphon funds from victims.

- **DarkComet:** DarkComet is a remote administration tool (RAT) that, while having legitimate purposes for remote system management, was often used by hackers for malicious intent. It allowed unauthorized access and control of infected systems, enabling spying and data theft.

- **Poison Ivy:** Another RAT, Poison Ivy, allowed attackers to gain remote access to infected systems, giving them control over file transfers, keystrokes, and even the ability to turn on webcams or microphones for surveillance purposes.

Antivirus

Definition:

Antivirus software (computer protection software) is a program(s) that is created to search, detect, prevent and remove software viruses from your system that can harm your system. Other harmful software such as worms, adware, and other threats can also be detected and removed via antivirus. This software is designed to be used as a proactive approach to cyber security, preventing threats from entering your computer and causing issues. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks.

Uses of Antivirus:

- **Malware Detection and Removal:** Antivirus programs are designed to detect, quarantine, and remove malware from computers and devices. They scan files, applications, emails, and other content to identify known signatures or behaviors of malicious software.

- **Real-time Protection:** Antivirus software provides real-time protection by constantly monitoring system activities. It actively scans incoming files and network data to prevent malware from infiltrating the system.

- **Vulnerability Detection:** Some advanced antivirus programs can identify and alert users about potential security vulnerabilities in their systems, such as outdated software or unpatched applications that might be exploited by cyber attackers.

- **Web Protection:** Many antivirus solutions include features to safeguard users while browsing the internet. They can block access to malicious websites, prevent phishing attempts, and alert users about potentially harmful links.

- **Email Protection:** Antivirus software scans incoming and outgoing emails for malware, attachments, or links that might contain threats. It helps prevent users from inadvertently downloading or opening malicious content.

- **Performance Optimization:** Some antivirus tools include system optimization features to enhance device performance by cleaning up unnecessary files, managing startup programs, or optimizing system settings.

- **Scheduled Scans and Updates:** Antivirus programs often allow users to schedule regular scans and updates to ensure that the software is up-to-date with the latest virus definitions and security patches.

- **Behavioral Analysis:** Advanced antivirus solutions use behavioral analysis and heuristic scanning to identify new or unknown threats based on suspicious behaviors, even if they don't match known malware signatures.

- **Data Protection:** Some antivirus software includes encryption or file-locking features to protect sensitive data from unauthorized access or ransomware attacks.

Example:

- **Norton Antivirus:** Norton by Symantec offers comprehensive protection against viruses, malware, ransomware, and other online threats. It provides real-time protection, a wide range of scanning options, and additional features like a firewall and password manager.

- **McAfee Antivirus:** McAfee is known for its robust antivirus solutions offering real-time protection against viruses, spyware, and ransomware. It includes features such as web protection, firewall, and performance optimization tools.

- **Bitdefender** Antivirus: Bitdefender offers powerful antivirus solutions known for their high detection rates and minimal system impact. It provides advanced threat defense, web protection, and ransomware remediation features.

- **Kaspersky Antivirus:** Kaspersky is renowned for its comprehensive antivirus and internet security solutions. It offers real-time protection against viruses, phishing attempts, spyware, and other online threats, along with features like a virtual keyboard for secure data entry.

- **Avast Antivirus:** Avast provides free and premium antivirus software with a strong focus on real-time protection against malware, ransomware, phishing attacks, and other threats. It includes additional features like a Wi-Fi inspector and password manager.

Social Engineering

Definition:

Social engineering is a manipulation technique that exploits human error to obtain private information or valuable data. In cybercrime, the human hacking scams entice unsuspecting users to disclose data, spread malware infections, or give them access to restricted systems. Attacks can occur online, in-person, and by other interactions. Social engineering scams are based on how people think and act.

Types of Social Engineering:

There are many different types of social engineering attacks, each of which uses a unique approach to exploit human weaknesses and gain access to sensitive information. Here are some of the types of attacks, include:

1. **Phishing:** Phishing is a type of social engineering attack that involves sending an email or message that appears to be from a legitimate source, such as a bank, in an attempt to trick the recipient into revealing their login credentials or other sensitive information.
2. **Baiting:** Baiting is a type of social engineering attack that involves leaving a tempting item, such as a USB drive, in a public place in the hope that someone will pick it up and plug it into their computer. The USB drive is then used to infect the computer with malware.
3. **Tailgating:** Tailgating is a type of social engineering attack that involves following an authorized individual into a secure area, such as a building or data center, without proper authorization.
4. **Pretexting:** Pretexting is a type of social engineering attack that involves creating a false identity or situation in order to trick an individual into revealing sensitive information. For example, an attacker might pretend to be a customer service representative in order to trick an individual into giving them their login credentials.
5. **Vishing:** Vishing is a type of social engineering attack that involves using voice phishing, or "vishing," to trick individuals into revealing sensitive information over the phone.

Example of Social Engineering:

1. **Business Email Compromise (BEC)**

BEC is also sometimes called 'CEO fraud' or 'Whaling'. Whaling emails are a form of spear phishing emails that usually involve someone masquerading as a senior level executive like a CEO, CSO or COO asking another employee, in the finance department for example, to transfer money to a vendor, partner or outside third-party entity.

The objective of this scam is to trick a company into moving large sums of money to a fraudster's bank account. BEC cost 20,373 individual U.S. businesses around $1.2 billion in 2018, according to the FBI's Internet Crime Report (ICR). The typical sub-components of the scam involve surveillance on a target company/employee(s), by building a relationship with certain employees using email, phone calls, and similar, or spoofing a CEO or similar C-Level email account, and tricking an employee into moving large sums of money to a fraudster's account. BEC may or may not involve using hacking techniques such as email account compromise.

2. **Phishing**

According to Proofpoint's State of the Phish Report 2019, 83% of companies in 2018 were targeted by a phishing campaign. The targeted form of phishing, spear phishing, was experienced by 64% of companies. Phishing via email, mobile device (SMShing) or phone call (Vishing) remains a highly successful vector with phishing being the main method used to initiate a data breach.

3. **Watering Hole**

Watering hole attacks are the ultimate attack based on surveillance of the target company. The attack's ultimate goal is to either steal privileged user login credentials or infect a network with malware. The cybercriminal(s) behind the attack will learn which websites the subjects visit most often. They then search for vulnerabilities in the website. If found, they will exploit the flaw, creating a trap, and wait for the target to visit the site. Once they do, malicious code can be injected into the source network and malware infection is carried out.

Website Security Consideration

Definition:

"Website security considerations" refer to the various factors and measures taken to protect a website from cyber threats, unauthorized access, data breaches, and other security risks. These considerations encompass a range of practices, protocols, and strategies implemented to safeguard the confidentiality, integrity, and availability of a website and its data.

Security Considerations:

Updated Software

It is mandatory to keep you software updated. It plays vital role in keeping your website secure.

SQL Injection

It is an attempt by the hackers to manipulate your database. It is easy to insert rogue code into your query that can be used to manipulate your database such as change tables, get information or delete data.

Cross Site Scripting (XSS)

It allows the attackers to inject client side script into web pages. Therefore, while creating a form It is good to endure that you check the data being submitted and encode or strip out any HTML.

Error Messages

You need to be careful about how much information to be given in the error messages. For example, if the user fails to log in the error message should not let the user know which field is incorrect: username or password.

Validation of Data

The validation should be performed on both server side and client side.

Passwords

It is good to enforce password requirements such as of minimum of eight characters, including upper case, lower case and special character. It will help to protect user's information in long run.

Upload files

The file uploaded by the user may contain a script that when executed on the server opens up your website.

SSL

It is good practice to use SSL protocol while passing personal information between website and web server or database.

Secure Socket Layer and Transport Layer Security

SSL stands for Secure Socket Layer while TLS stands for Transport Layer Security. Both Secure Socket Layer and Transport Layer Security are the protocols used to provide security between web browsers and web servers. The main difference between Secure Socket Layer and Transport Layer Security is that, in SSL (Secure Socket Layer), the Message digest is used to create a master secret and it provides the basic security services which are Authentication and confidentiality. While In TLS (Transport Layer Security), a Pseudo-random function is used to create a master secret.

There are some differences between SSL and TLS which are given below:

SSL	TLS
SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.
SSL (Secure Socket Layer) supports the Fortezza algorithm.	TLS (Transport Layer Security) does not support the Fortezza algorithm.
SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
In SSL(Secure Socket Layer), the Message digest is used to create a master secret.	In TLS(Transport Layer Security), a Pseudo-random function is used to create a master secret.
In SSL(Secure Socket Layer), the Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
SSL (Secure Socket Layer) is more complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.
SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security).	TLS (Transport Layer Security) provides high security.

Digital Signatures and Digital Certificate

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

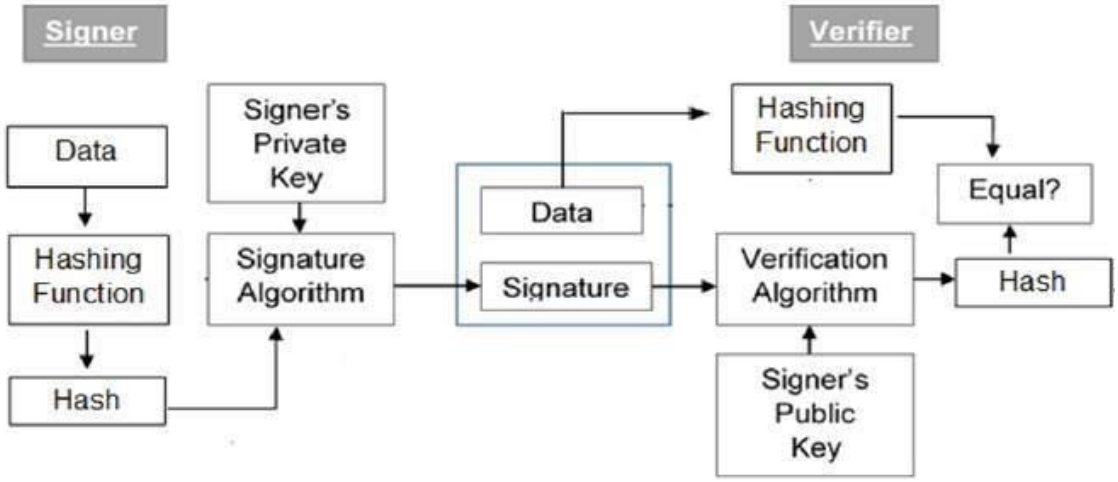
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –



The following points explain the entire process in detail –

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature –

- **Message authentication –** When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

- **Data Integrity –** In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

- **Non-repudiation –** Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely – Privacy, Authentication, Integrity, and Non-repudiation.

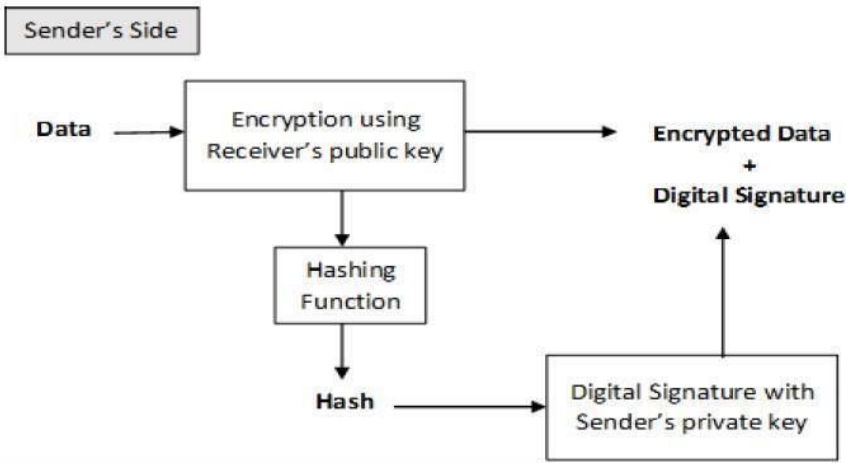
Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are two possibilities, sign-then-encrypt and encrypt-then-sign.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration –



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.