Table of Contents

ABSTRACT 5

INTRODUCTION TO SECURITY OF NETWORKS 6

HISTORY OF SECURITY OF NETWORKS 7

Threats From the Seven OSI Model 8

a. Layer-1 9

b. Layer-2: 9

c. Internet TCP/IP 9

d. Shipping class 9

e. Session class 9

f. Presentation layer 9

g. Application class: 9

a. White hat 10

b. Black hat 10

c. Children's Scenario 10

d. State-sponsored cyberattacks: 10

e. Heckerism 10

TYPES OF SECURITY OF NETWORK 11

SECURITY OF NETWORK ACTIVE ATTACKS 11

a. Malware 11

b. Ping of death 11

c. Machine-in-the Middle 11

d. Phishing 11

NETWORK SECURITY PASSIVE ATTACK 12

a. Email mimicking 12

b. Password heists 12

c. Rainbow table attack 12

d. Shoulder surfing 12

e. Caller ID Spoofing 12

f. DNS Spoofing 12

g. Wormhole 12

h. Fabrication 12

i. Sinkhole 12

j. Sybil 12

k. Traffic analysis 13
l. Eavesdropping 13
m. Monitoring 13
n. Advanced attacks 14
o. Black hole attack: 14
p. Rushing attack 14
q. Replay attack 14
r. Byzantine attack: 14
s. Location disclosure attack: 14
t. Black hat attacks 14
u. Malware attacks 15
v. Phishing attacks: 15
w. DDoS incidents 15
SECURITY OF NETWORK CONTROLS 16
a. Intrusion Detection System 16
b. Virtual Private Network 16
c. Data Encryption 16
INTRODUCTION TO CRYPTOGRAPHY 18
TYPES OF CRYPTOGRAPHY 19
a. Private-key cryptography 19
Fig2: Private-key cryptography 20
b. Public-Key Cryptography 21
Fig3: Public-key cryptography 21
TYPES OF PUBLIC-KEY ENCRYPTOGRAPHY 23
a. Encryption model 23
b. Plaintext 23
c. Encryption Algorithm: 24
d. Ciphertext ..... **Error! Bookmark not defined.**
e. Decryption Algorithm ..... **Error! Bookmark not defined.**
f. Encryption Key 25
g. Decryption Key 25
h. Algorithm 25
COMMON ENCRYPTION ALGORITHMS 26
c. RSA: Rivest, Shamir, and Adleman 26

d. Hashing 26
e. Message Digest Algorithm 5 26
g. Advanced Encryption Standard .... **Error! Bookmark not defined.**
h. Secure Hash Algorithm 1 .... **Error! Bookmark not defined.**
i. Hash-based Message Authentication Code 27
REPEATED DENITION OF SERVICE 32
Fig3. Exploitation of Denial of service 33
Fig3. Exploiting Protocol Features in Application Layer DDoS Attacks 35
SYMPTOMS OF DDoS ATTACKS 36
a. Slow network performance or unresponsiveness 36
b. Increased spam emails 36
c. Unusual traffic patterns 37
d. Inability to access websites. 37
e. Increased latency 37
f. Outages 37
g. Network congestion 37
HOW DOES DISTRIBUTED DENIAL OF SERVICE WORKS 38
Fig 3. DDoS Cloudflare 39
a. Volume attacks 40
b. TCP State-Exhaustion attacks 40
c. Application Layer attacks 41
d. HTTP Flood 41
e. DNS Flood 41
f. DDoS Botnet 41
g. Application-layer protocol attacks 41
h. Protocol attacks 41
TRANSPORT LAYER 43
a. SSL/TLS Flood 43
b. SSL/TLS renegotiation attack 43
c. SSL/TLS handshake attack 43
d. Encrypted DDoS attacks 44
TYPES OF DDoS ATTACKS 45
Single IP single port 45
Single IP multiple port 45

SCOPES AND OBJECTIVES 49
Authenticity 50
Integrity 50
FUCNTIONALITY OF ADVANCED ENCRYPTION STANDARD (AES) 52
Key Expansion 52
Initial Round 52
Rounds 53
Final Round 53
THEORETICAL RESULT OF CRYPTOGRAPHY AND NETWORK SECURITY 55
RECOMMENDATIONS 56
IMPLICATIONS OF THEORY AND PRACTICE 57
a. Framework for Research 57
b. Evaluation of Existing Methods 57
c. Identification of Research Gaps 57
d. Development of New Methods 57
e. Standardization of Methods 57
APPENDIX A 58
Resources for Cryptography and Network Security in Online Research 59
References 60

ABSTRACT

Network Security involves using cryptography to ensure the confidentiality of data during data transmission both wired and wireless connections.

Data Security is crucial for secure transmission for both dependable and unreliable over networks, with authorization of access controlled by the network administrator.

Network Security is utilized in various sectors such as private and public computer networks in organizations, enterprises, and institutions. The task of network security is not only limited to securing end systems but extends to the entire network topologies.

The CIA triad which is confidentiality, Integrity, and Availability plays important in protecting computer systems for who is whom the information is intended throw secure and available it maybe possibly to the data and how legitimate the information access. The implementation of network security is crucial for various government agencies, organizations, enterprises, banks, and businesses, as well as IoTs and our day-to-day communications.

Cryptography is an essential technology for network security as it allows us to receive messages comprehensively from the authorized recipient who possesses the decipher key. Cryptography is achieved using hash functions, a mathematical representation of the information that is calculated by the receiver upon message arrival. It is an emerging technology that is crucial for securing data.

In the past, cryptography was used to secure military information and diplomatic correspondence to protect national security, but its usage was limited. However, with the development of communication, the range of cryptography applications has expanded significantly.

Cryptography is essential for protecting data, making it a powerful tool for data security ensuring data security in modern times.

Cryptography is a way to use secure communication in such a way that an original message is transformed into an unreadable format, known as ciphertext, using mathematical algorithms. This process is called encryption, and it ensures that only authorized recipients can access the original message. The transformation process is reversible using a secret key or password, known as decryption.

Utilizing a variety of approaches, including symmetrical encryption with keys, and asymmetrically encrypted key encryption, cryptography ensures the confidentiality of the data being conveyed. In symmetric key encryption, the same key is used for decryption as well as encryption, whereas in asymmetric key encryption, unique keys are used for both encryption and decryption.

Data integrity, or the assurance that the data was not changed during transmission, is another goal of cryptography, and it is achieved through the use of hashing techniques.

Hash functions are one-way mathematical methods for transforming the original message into a fixed-length character string known as a hash, which is then stored in a database. Any changes made to the original message during transmission will result in a new hash value, maintaining data integrity.

INTRODUCTION TO SECURITY OF NETWORKS

Network security protects our organization and information from breaches, disruptions, and other dangers. Often an endless term, it includes all descriptions of arrangements of computer equipment and programs as well as forms or rules and configurations related to the use of arrangements, openness, and security. risk in general.

Networking security including takeover, anti-virus computer programs, application security, organization scanning, and network-related security types (endpoints, web application security frameworks, remote control, firewall encryption, endpoint locators, interrupt detection frameworks, and associated risk management). Sort security is an essential component of data security since it ensures the security of the sorting facility.

Organizational security refers to the capabilities, characteristics, strengths, operating procedures, responsibilities, measures, takeovers, and regulatory and administrative approaches of the required computer equipment and programs. to provide an adequate level of protection for equipment and programs within an organization.

Organizational security and cryptography can be a concept of organizational security and the transmission of information about an organization. Facility security often depends on layers of protection and includes various components including orchestration verification and extended computer program security for devices and machines. A security framework can be an organization's security utility that helps filter and channel an organization's outreach and activities based on an organization's existing security practices.

Together, all of the parts improve overall computer security. Through the use of cryptography, information security can be guaranteed.

The art and science of creating cryptic codes is known as cryptography. Protecting computer systems and the components that make them up against unauthorized access, use, disclosure, disruption, alteration, or destruction is the focus of security organizations. This includes updating different safeguards and inventions including firewalls, sporadic localization, encryption, and virtual private networks, which stop cyberattacks. Non-repudiation provides the ability to determine whether or not a person has undertaken a specific activity, such as creating data, sending messages, approving in giving data, or accepting messages, and protects against dishonest disclaimers who have done so.

The purpose of organized security is to secure the confidentiality, integrity, and availability of organized assets, measurement information, utilities, and applications. Confidentiality indicates that only authorized individuals or executives have access to sensitive information. The term judgment relates to the accuracy and consistency of knowledge, whereas accessibility suggests that organized assets are opened when needed.

Effective organizational security necessitates a comprehensive strategy that involves both preventative and remedial actions. Precautionary measures are intended to forecast the existence of security breaches, whilst corrective measures are intended to respond to security phases and mitigate their impact. Infections, malware, phishing assaults, do-it-yourself attacks, and ransomware are some of the most common organized security threats.

Businesses must put strong security procedures in place, educate staff members about best practices, and make use of cutting-edge security innovations to guard and disregard these threats.

HISTORY OF SECURITY OF NETWORKS

The foundation of network security is permission, which often entails a login and password. The network administrator implements policies and methods to prevent unauthorized access, modification, misuse, or denial of network resources. Access to data within the network is managed, and a security mechanism is employed to limit user access to specified services. Anti-virus software or an Intrusion Detection System are also used to detect and neutralize malware. The monitoring of network traffic using anomaly detection is logged for auditing and additional analysis. To protect the privacy of communication between two hosts on a network, encryption techniques can be applied.

With the increasing interconnectedness of the world through the Internet and IoTs, the security of network infrastructures has become critical. It is essential to research the history of network security, the security aspects of Internet architecture, types of network attacks, their corresponding security methods, and current developments in network security hardware and software. However, a communication gap between developers of network technology and security technology results in a lack of easily implementable security methods.

Network attacks fall into two categories: "Passive," in which the attacker just intercepts data, and "Active," in which the attacker launches orders to obstruct regular data flow. Spoofing, modification, denial of service, sinkhole, and Sybil assaults are examples of current attacks. Traffic analysis, eavesdropping, and monitoring are examples of passive assaults.
Advanced assaults include black hole attacks, rushed attacks, and replay attacks. Network assaults can affect network performance, result in uncontrolled traffic, and introduce viruses, it is vital to know. Last but not least, bad nodes might utilize the location disclosure attack to gather data on other nodes and attack routes.

The Open Systems Interconnection (OSI) paradigm is frequently used for designing networks. It offers modularity, usability, adaptability, and established protocols, all of which may be coupled to quickly build stacks for modular development. The seven OSI levels are as follows:

Threats From the Seven OSI Model

a. **Absorption layer dangers:**

DDoS attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris assaults are a few examples of application layer attacks.

Most businesses have a variety of abstraction layer security protections in place, such as web application firewalls (WAFs), secure web gateway services, and others, to combat these and other risks.

b. **Dangers in the syntactic layer.**

The most prevalent threats in the syntax layer are the SSL encryption packet resource intensive, attacker uses SSL tunnel HTTP attacks to target vulnerable servers.

In mitigating these attacks or consequences in SSL the main infrastructure and inspecting application traffic should not violate the policy of the application delivery platform (ADP).

A good ADP will always ensure the traffic in the presentation should forwarded whatever traffic is re-encrypted to the original infrastructure.

c. **Layer-5 threats**

A Telnet server running on the switch is vulnerable to DDoS attacks, which makes Telnet services unavailable.

d. **Transport layer threats:**

It uses transport layer security (TLS) to secure all communications between their Web servers and browsers, regardless of whether sensitive data is being transferred. TLS is a cryptographic protocol that secures network communications from start to finish. It is commonly used for internet communications and online transactions.

e. **Layer-2 threats:**

The data link layer ensures that data is transmitted securely across a physical connection. The network topology, network access, error notification, ordered frames-per-second transmission, flow management, physical rather than intellectual connecting with, and error communication are all a part of the data connection layer. Sniffing, spoofing, broadcast storms, and insecure or nonexistent virtual LANs (VLANs, or lack thereof) are a few examples of frame-level exploits and vulnerabilities. Misconfigured or broken network interface cards (NICs) can cause a network segment or the entire network to fail.

7 OSI MODEL

The Open Systems Connectivity Model is a theoretical framework designed to assist standardize network communications. It is made up of seven levels, each with its own set of functions and protocols that allow devices to communicate with one another.
The seven levels of the OSI model are as follows:

a. **Layer-1**: Is in charge of sending unprocessed data bits via a physical medium, such as copper wire, fiber optic cable, or a wireless signal. It details the physical characteristics of the communication channel, including the voltage level, signaling rate, and transmission range.
b. **Layer-2:** This layer guarantees that data frames are reliably sent between network nodes. By providing error recognition and repair code, managing the movement of information, and granting accessibility to the physical layer, it guarantees mistake-free information transfer.
c. **Internet TCP/IP**: This layer is responsible for transmitting packets from one network node to the next. It employs routing technologies such as the Internet Protocol to determine the best path for data transfer.

d. **Shipping class**: This layer guarantees dependable end-to-end data transmission across applications running on different network servers. It ensures that information is transmitted accurately, in the right order, and without loss or duplication.

e. **Session class**: This layer creates, maintains, and ends sessions between applications operating on various servers. It provides authentication, authorization, plus services for encryption to enable safe communication.
f. **Presentation layer**: This layer converts data between application and network formats. It conducts data compression, encryption, and decryption to guarantee that data is transferred in a format that the recipient application can comprehend.

g. **Application class:** This layer provides services that allow end users to access network resources, such as email, web pages, and file transfers. It includes application protocols, such as HTTP, SMTP, and FTP.

HACKERS: TYPES

Individuals or groups of individuals who use their computer knowledge and skills to gain unauthorized access to computer systems and networks.

They can do this for a variety of reasons, such as stealing sensitive data, spreading malware, defacing a website, or simply because of the act's own disregard and notoriety.

a. **White hat**: These are also known as ethical hackers, and they use their skills to do good by helping organizations identify and fix vulnerabilities in their systems.

b. **Black hat** : They are hazardous hackers who employ their expertise for nefarious purposes, such as stealing information or cash, wrecking computer systems, or disseminating malware. hackers that use tactics that lie midway between white hat and black hat are known as gray hat.
They can perform unlawful operations to detect system vulnerabilities, but they cannot always gain authorization from the system owner to do so.

c. **Children's Scenario**: These are individuals with limited technical skills that use predefined tools and scripts to launch attacks.

d. **State-sponsored cyberattacks:**
To obtain information about other nations, the government hires hackers. State-sponsored hackers are those that operate in this manner. They employ their expertise to obtain sensitive information from foreign nations in order to adequately foresee any threats to their nation. Sensitive information assists in not just managing current crises but also averting potential problems in the future. All of their reporting is to their government.

e. **Heckerism**: Is it hacking or hacking into computer systems, for political purposes or social motives.

TYPES OF SECURITY OF NETWORK

Here, we're going to go through some fundamental categories of assaults that might lead to issues with unrestrained traffic, malware, and sluggish network performance. Attacks on the network from malicious nodes can be divided into two types: "Passive" attacks, meaning that the intruder intercepts data passing through the network, and "Active" attacks, in which the intruder initiates commands to interfere with the network's normal operation.

SECURITY OF NETWORK ACTIVE ATTACKS

An active attack is a type of security breach in which an unauthorized person or entity attempts to alter, destroy, steal, or insert data into a system or network. Unlike passive attacks, which involve monitoring or eavesdropping on data, active attacks involve actively manipulating or interfering with data in some way. Active attacks can be more dangerous than passive attacks, as they involve a direct attempt to interfere with or harm a system or network.

a. Malware

A sort of software known as malware is intended to damage or exploit a computer system. Data theft, file corruption, and computer takeover are all possible with malware.

b. Ping of death

A DoS attack involves flooding a system or network with traffic in order to overwhelm it and make it unavailable to users. This can prevent legitimate users from accessing the system or network.

c. Machine-in-the Middle

In a MitM attack, an attacker intercepts communications between two parties and inserts themselves into the conversation. The attacker can then eavesdrop on the conversation, steal data, or manipulate the data being transmitted.

d. Phishing

Phishing is a type of social engineering attack in which an attacker sends an email or message that appears to be from a trusted source in order to trick the recipient into divulging sensitive information, such as passwords or credit card numbers.

NETWORK SECURITY PASSIVE ATTACK

An inactive cyberattack is one in which the hacker only intercepts and keeps track of the data moving through a network without making any changes or modifications. Passive attacks seek illegal access to sensitive or secret data such as passwords, credit card numbers, or personal information. A form of virus known as ransomware encrypts a victim's files and demands money in exchange for the decryption key.

a. **Email mimicking**: Is the act of transmitting an email from a false email address that looks to be from a reliable source. This can be used to dupe the receiver into disclosing sensitive information or clicking on a malicious link.

b. **Password heists**: Password assaults are a sort of cyberattack that seeks to obtain unauthorized access to a user's account or system by guessing or breaking their password. Password assaults can be classified into numerous kinds, including:

c. **Rainbow table attack**: This attack involves using precomputed tables of encrypted passwords to quickly determine the plaintext password. Rainbow table attacks are faster than brute force attacks because they do not have to compute the hashes in real-time.

d. **Shoulder surfing**: This attack involves watching someone enter their password and memorizing it for later use. Shoulder surfing attacks can be successful in public places or shared workspaces while this attack is not necessarily active.

e. **Caller ID Spoofing**: Caller ID spoofing involves falsifying the caller ID information displayed on a recipient's phone to make it appear as if the call is coming from a trusted source. This can be used in voice phishing (vishing) attacks or to hide the caller's true identity.

f. **DNS Spoofing**: Domain Name Server spoofing involves falsifying DNS records to redirect a user to a malicious website or to intercept their network traffic. This can be used in phishing attacks or to launch man-in-the-middle attacks.

g. **Wormhole**: Is a type of network attack that allows an attacker to create a shortcut or tunnel between two distant points on a network. It is a serious security threat that can be exploited by attackers to intercept, modify, or redirect network traffic.

h. **Fabrication**: Fabrication refers to the creation of false information or data. Fabrication attacks involve the deliberate and unauthorized insertion or modification of data in a computer system or network to deceive the system or its users.

i. **Sinkhole**: A sinkhole, in the context of computer networking and cybersecurity, refers to a technique used to redirect traffic from its intended destination to a malicious destination.

j. **Sybil**: Sybil attack is a type of attack in which an attacker creates multiple fake identities or personas to gain control over a network or system.
The Sybil attack is typically used in peer-to-peer networks or decentralized systems to disrupt the normal functioning of the network by flooding it with fake identities or controlling the majority of nodes in the network.

In a peer-to-peer file sharing network, an attacker can create multiple fake identities and flood the network with fake files, making it difficult for users to find genuine files. Similarly, in a decentralized cryptocurrency network, an attacker can create multiple fake identities and control the majority of the nodes, allowing them to manipulate the network and potentially conduct fraudulent transactions.
The term "Sybil attack" was coined by computer scientist John R. Douceur in 2002, and it is named after the famous case of a woman with dissociative identity disorder who claimed to have over sixteen different personalities.

k. **Traffic analysis**: Is a passive attack where an attacker attempts to gain information about the communication path between the sender and the receiver by analyzing the traffic on the network. This attack does not involve modifying the data being transmitted, but instead, the attacker tries to determine the amount of data that is being transferred, the frequency of the communication, and the identities of the communicating parties.
The attacker may also try to identify patterns in the traffic that can reveal sensitive information, such as the nature of the communication or the type of data being transmitted. Traffic analysis can be used by an attacker to infer sensitive information about the communication, such as user behavior, preferences, and intentions. For example, an attacker can infer that two parties are communicating regularly and may be involved in a confidential transaction. The attacker may also identify patterns in the traffic that can reveal the type of communication taking place, such as whether it is a voice call or a video conference. To prevent traffic analysis attacks, encryption and anonymity techniques can be used.

Encryption techniques can be used to protect the confidentiality of the communication by encrypting the data before it is transmitted.
Anonymity techniques can be used to protect the identity of the communicating parties by masking their IP addresses or other identifying information.

l. **Eavesdropping**: Eavesdropping is a type of passive attack that occurs in wired and wireless networks. In this attack, the attacker tries to secretly listen in on the communication between the sender and receiver in order to obtain confidential information. The attacker may try to obtain private or public keys of the sender or receiver, or any other secret data being transmitted between them.

m. **Monitoring**: Monitoring is a type of passive attack in which an attacker can observe the communication between the sender and receiver without modifying or altering the data being transmitted. The attacker can read the confidential data being communicated but cannot modify it.

This type of attack can be used to gather sensitive information such as passwords, account information, and other confidential data. Monitoring can be done by using various tools and techniques such as packet sniffers, network analyzers, and protocol analyzers. It is important to secure communication channels and use encryption techniques to prevent monitoring attacks.

n. **Advanced attacks**: Advanced attacks refer to sophisticated and complex cyber-attacks that are designed to evade traditional security measures and exploit vulnerabilities in an organization's systems or applications.
These attacks often involve the use of advanced techniques, such as malware, social engineering, and zero-day exploits, to gain unauthorized access to sensitive information or systems.
Advanced attacks are typically conducted by highly skilled and motivated attackers, such as state-sponsored hackers, cybercriminals, and hacktivists, who have significant resources and expertise at their disposal. These attackers may use a variety of tactics to breach an organization's defenses, including targeted phishing emails, social engineering, and advanced malware that can bypass traditional antivirus software.

The consequences of advanced attacks can be severe, ranging from the theft of sensitive information to the disruption of critical infrastructure. To protect against these threats, organizations must adopt a multi-layered approach to security that includes advanced threat detection and response capabilities, regular security awareness training for employees, and ongoing security monitoring and testing.

o. **Black hole attack:**
In this kind of assault, the perpetrator presents himself as possessing the best route to the node whose packets he wishes to intercept. The attacker lists the initiator's request for a route using a flooding-based protocol, then generates a reply message claiming to have the shortest way to the recipient. The initiator will regard the communication from the attacker to be the fastest way to the recipient because it arrives before the response from the real node, resulting in a malicious false route.

p. **Rushing attack**: In a rushing attack, the attacker modifies the packet sent by the sender to the receiver and sends a duplicate to the receiver repeatedly, keeping the recipient busy.

q. **Replay attack**: A malicious node could repeat or lag the data sent between nodes during this kind of attack. To obtain passwords or other sensitive information, the attacker intercepts the data and retransmits it.

r. **Byzantine attack:** In a Byzantine assault, a number of intermediary nodes operate between the sender and receiver and adjust, such as forming routing loops, sending packets through less-than-ideal pathways, or arbitrarily discarding packets, which can impair or disrupt routing services.

s. **Location disclosure attack:** In this type of attack, a malicious node collects information about the nodes and the route by computing and monitoring the traffic. The malicious node can use this information to perform further attacks on the network.

t. **Black hat attacks**: Refer to malicious cyber-attacks conducted by hackers or cybercriminals with the intention of compromising, damaging, or stealing data or systems. These attacks are often illegal and unethical and are conducted with the aim of personal gain, financial benefit, or causing harm to an individual, organization, or country.

u. **Malware attacks**: Malware refers to any malicious software that is designed to harm or compromise computer systems. Black hat attackers often use malware to steal sensitive data, spy on users, or gain unauthorized access to systems.

v. **Phishing attacks:** Phishing attacks utilize phony emails or messages to deceive users into divulging private information like passwords, credit card numbers, or other personal information.

w. **DDoS incidents**: Distributed Denial of Service attacks include flooding a website or online service with traffic from numerous sources, rendering it inaccessible to authorized users.

(J, 22 May 2015)

SECURITY OF NETWORK CONTROLS

a. Intrusion Detection System

An Interruption Discovery Framework could be a security innovation outlined to distinguish and react to pernicious action on computer frameworks and systems.

The system monitors network activity and framework occasions, seeking out for signs of suspicious behavior which will show an assault or interruption endeavor.

A host-based IDS is introduced on individual systems, checking action on that particular gadget, whereas a network-based IDS is introduced on the organize, observing activity on the whole organization. DS employments an assortment of procedures to identify pernicious movement, counting signature-based location, which compares arrange activity or framework occasions against a database of known assault marks, and anomaly-based location, which looks for deviations from anticipated behavior.

Once an IDS recognizes an assault, it produces an alarm or takes activity to anticipate the assault from succeeding. A few IDS can too be arranged to naturally react to recognized assaults by blocking activity, ending forms, or other measures.

b. Virtual Private Network

A Virtual Private Organize may be an innovation that makes a secure and private association between two or more gadgets over the web. It gives a way for farther clients or department workplaces to safely get to a company's private arrange or the web, by making a virtual "burrow" between the user's gadget and the VPN server.

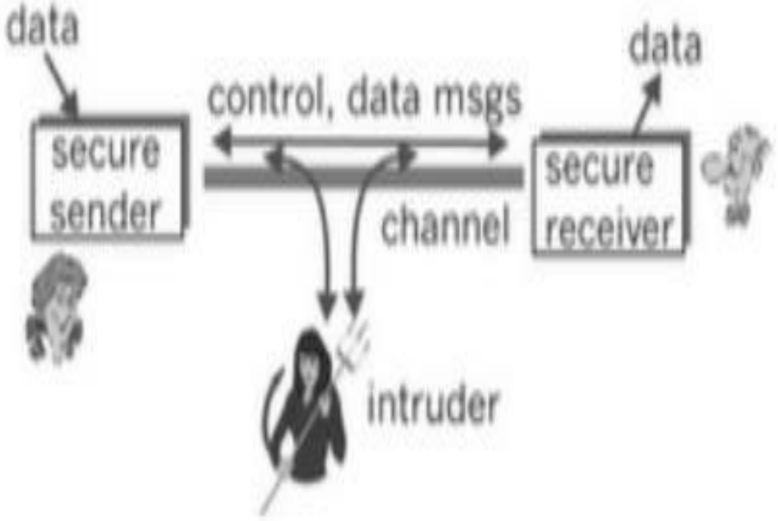
The VPN innovation scrambles all the information that passes through the burrow, making it troublesome for programmers, ISPs, or other entities to intercept or peruse the activity. VPNs utilize distinctive conventions to set up the secure association, such as SSL/TLS, IPsec, PPTP, L2TP, or OpenVPN.

VPNs are utilized for an assortment of purposes, such as further getting to a company's arrange, bypassing web censorship and geo-restrictions, improving online protection and security, and anticipating malevolent assaults like man-in-the-middle assaults.

Whereas VPNs give improved security and protection, it is vital to select a trustworthy VPN supplier and arrange it appropriately to dodge any potential vulnerabilities.

c. Data Encryption

Data encryption is the process of converting plain or unencrypted data into a coded or encrypted form to ensure that the information remains confidential and secure. Encryption uses algorithms and keys to convert the data into a scrambled format that cannot be read by anyone without the correct decryption key.


data
control, data msgs
data
secure sender
channel
secure receiver
intruder

INTRODUCTION TO CRYPTOGRAPHY

Cryptography is used to represent something secure, secret, cryptic, or obfuscated. Encryption is considered a numerical strategy for securely sending private girlfriend messages through dubious channels. Encryption is a fundamental method of protecting data from various types of intruders such as impedance, tampering, and tampering, and has been around for about 2000 years. They shaved their slaves' heads, tattooed messages on them, and grew their hair out. The main use of cryptography dates back to 1900 BC. return. to go back.

When Egyptian copyists used unusual symbolism in their etchings. Some experts argue that the cipher appeared soon after the document was written and that its use ranged from reconciliation memos to wartime battle plans. Shifts each character in a character set by the specified amount. It's fragile. Vigenère's polyalphabetic cipher is a generalization of Caesar's motion cipher. Scramble route selection requires a slogan. Substitution cipher:26-character level with word references. It's fragile. At this point, various cryptographic computations are performed within the given date, as described in the rest of this chapter.

Most modern cryptographic computations are based on the basic method of computing the extended integrability of prime numbers, which is considered difficult. In both symmetric and divergent cryptosystems, encryption is the process of transforming the primary form of matter into a complex form, whereas decryption involves extracting the primary form of data from unrelated matter. will be Secondary encryption uses plaintext and source code for analysis while keeping a large distance from data development.

This chapter describes protection. Encryption is the most important tool for ensuring security. The purpose of encryption is to ensure confidentiality, verification, and validity of information. Encryption is a secure communication method that achieves these goals by transforming plaintext (clear data), so to speak, into ciphertext (unintelligible data) visible to the intended recipient. The main purpose of confidentiality encryption is to ensure the protection of information. This is usually done routinely by encrypting information so that it cannot be viewed by unauthorized persons. Encryption is the conversion of plaintext into ciphertext using an encryption method and a puzzle key.

The ciphertext can be decrypted (converted to plaintext) by someone who has the key to the puzzle. insight: Encryption also ensures the identity of the data. This means that there is a guarantee that the information has not been altered or altered in any way.

This can be accomplished by using message authentication codes (MAC) or extended signatures. A MAC is a code created by cryptographic computation and a secret key used to ensure that a message has not been altered in transit. A computer signature is a code created by cryptographic computation and a private key that is used to verify that a message was sent by the person claiming to be the sender.

TYPES OF CRYPTOGRAPHY

a. Private-key cryptography

The same key is used for encryption and decoding in symmetric encryptions. Both the sender and the recipient have a replica of this key, which the sender uses to scramble the message immediately after it is transferred. At the time, the intended recipient used the same key to decipher the message and assess its substance. Symmetric encryption is frequently quicker and more efficient than halter kilter authentication since it requires smaller key dimensions. Nevertheless, it is necessary for the sender and the recipient to have gotten the same private key, which could be a challenge in some circumstances.

The security of any communications using that private key is also compromised if it is compromised.

In a symmetric key structure, everyone who wants to access the information has the same key. Keys for scrambling and decoding messages must also be kept secret to ensure data security.

While this may work, the safe distribution of keys required to ensure sufficient control renders symmetric encryption unsuitable for widespread commercial use. A common method to symmetric encryption is to characterize the process of encryption as a probabilistic or state-dependent operation with a message M and a key K. To generate the ciphertext, the encryption prepare can flip a coin or change the one they chose sentence pattern.

The encryption plot uses deterministic work to generate an initialization vector (IV). The client provides a message M, a key K, and an initialization vector in the following instance.

This key is duplicated by both the sender and the recipient and is used by both parties to scramble messages at the time of transmitting. Symmetric encryption is often faster and more effective than deviated encryption because it uses shorter key lengths. Nevertheless, it poses a few challenges in particular situations because both the sender and the recipient must have access to the same private key. Furthermore, if the private key is compromised, the security of all conversations using that key is jeopardized.

Keys for scrambling and decoding messages must also be kept confidential to ensure information security. While this may work, the safe distribution of keys required to ensure sufficient control renders symmetric encryption unsuitable for widespread commercial use.

A popular approach for symmetric encryption is to model encryption as a probabilistic or state-dependent activity with a message M and a key K. The encryption algorithm can tweak an alternate phrase composition or toss a piece of paper to produce the ciphertext C.

The encryption approach employs deterministic work in order to construct an initialization vector (IV). The client supplies a message M, a key K, and an initialization vector N, resulting in a specific ciphertext C = KN(M).

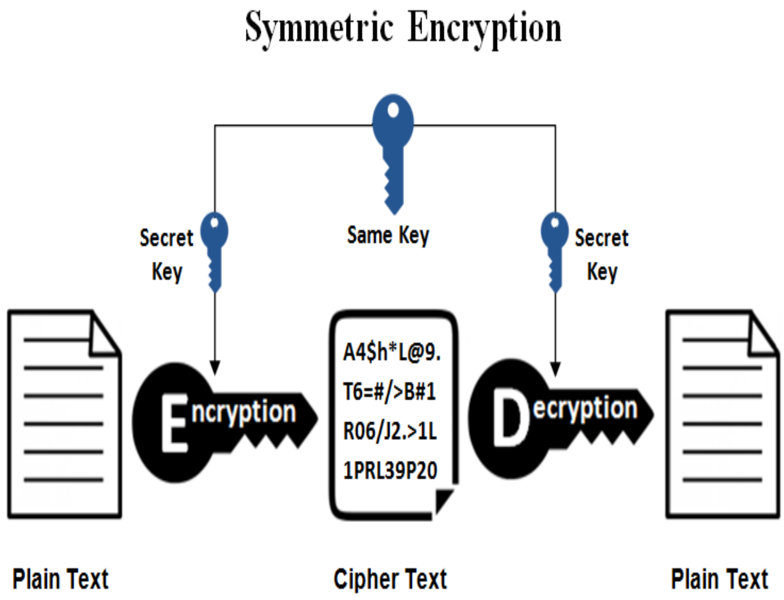


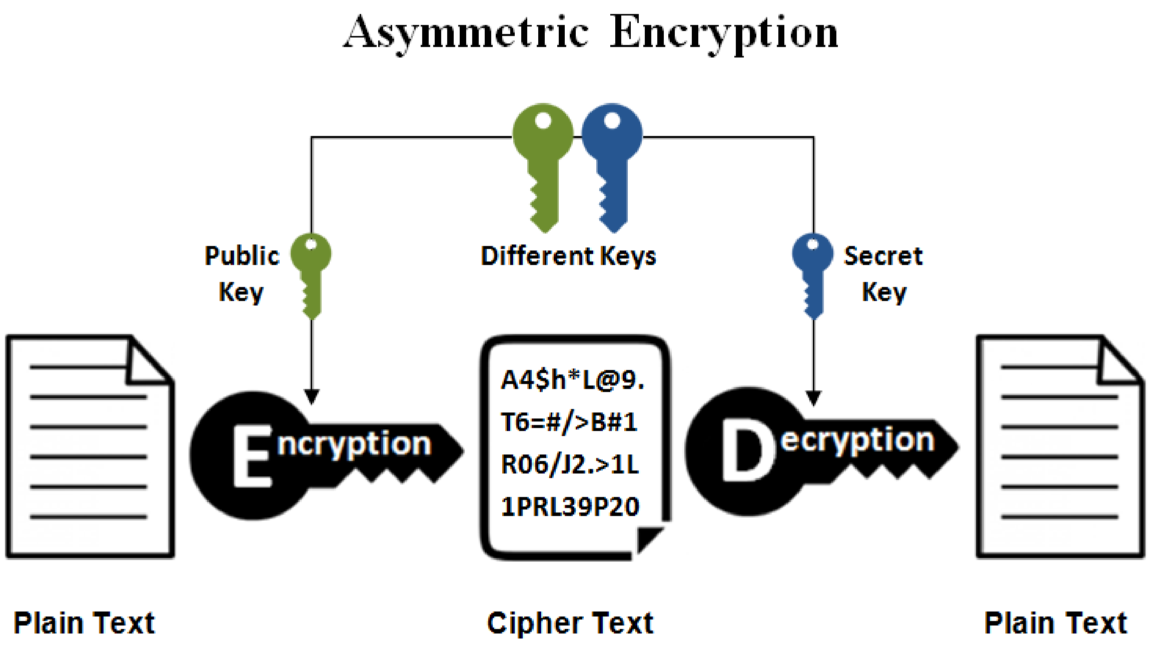
Fig2: Private-key cryptography

b. Public-Key Cryptography

Involves using different keys for encryption and decryption, as opposed to symmetric encryption, which utilizes the same key for both operations. One of the most popular techniques for encrypting data is Advanced, which is located Encryption Rules and Regulations, which employs block encryption for safeguarding data which includes discussions between administrations and financial transactions. This article focuses on nonce-based encryption, where the IV is assured to be a nonce that changes value with each encrypted message. We look at the definitions, structures, and characteristics of nonce-based encryption. By utilizing a surfacing IV, symmetric encryption more accurately represents actual structures like CBC mode, and encryption techniques created to be secure under nonce-based security principles are less prone to abuse.

These methods can aid in the detection and blocking of malicious traffic while allowing legal traffic to pass through and preserving stable network performance.
One of the most typical signs of a DDoS assault is this. Due to the high traffic the attacker has generated, the entire network may become slower or perhaps unusable.
(Anitha, January 2022), (Rogaway, 2004)

Fig3:Cryptography using public keys



Public key encryption is a secure method of communicating between two parties that makes use of two keys: a public key and a private key.
The public key is accessible to all and is used for encryption, but the private key is kept secret by the owner and is used for decoding. The sender obtains the recipient's public key and applies it to the message to encrypt it. Sending the recipient's private key after the message has been encrypted enables them to decrypt it.
The RSA algorithm is a popular public key encryption algorithm for securing online transactions, email communications, and other sorts of electronic communication.

Public key cryptography is also used to verify the authenticity of digital documents and messages. The sender's private key is used to encrypt a hash of the message, and the recipient uses the sender's public key to verify the signature. This maintains confidentiality and guarantees the network's security.
Public Key Encryption, often known as asymmetric encryption, is a cryptographic approach that uses two distinct but mathematically related keys - a public key and a private key - for data encryption and decryption.

The public key is shared with everyone, while the private key is kept private by the owner. When a message is sent to the owner, the public key is used to encrypt the message, which can only be decrypted with the private key. Only the owner of the private key will be able to read the message this way.
A vital technology for protecting online transactions, digital signatures, and secure communication over the internet, public key encryption is widely utilized in a number of security protocols, including SSL/TLS, SSH, and PGP.
.

TYPES OF PUBLIC-KEY ENCRYPTOGRAPHY

a. Encryption model

Encryption is a security technology that transforms plaintext or unencrypted data into ciphertext or encrypted data in order to secure its confidentiality, integrity, and validity. An encryption model describes the phases and procedures involved in encrypting and decrypting data, including the type of encryption algorithm, key generation and management, data encoding and decoding, and the security protocols utilized.

Depending on the particular system requirements, the kind of data being secured, and the required level of security, many encryption models could be used. Symmetric encryption, asymmetric encryption, hashing, digital signatures, and key management systems are a few examples of popular encryption models.

The same key is used in symmetric encryption for both data encryption and decryption. This sort of encryption is widely used to protect data during transmission, as via the internet. Asymmetric encryption, on the other hand, employs two keys: a public key for encrypting and a private key for decryption.

For secure communication, such as encrypted emails or digital signatures, this type of cryptography is often utilized.

Hash functions are used to convert data into a fixed-length string of characters known as a hash value. These values are used to confirm the accuracy of the data because they are specific to each input. Digital signatures, on the other hand, are used to authenticate the source of the data, ensuring that it has not been tampered with or modified during transmission.

Encryption keys are created, stored, distributed, and revoked using key management systems. As tampered keys may lead to tampered encrypted data, these systems are essential to the encryption model's security.

Encryption models, in general, are essential for safeguarding data and preventing illegal access, theft, or modification.

b. Plaintext*:*

Plaintext refers to the original message or data that is readable and understandable to humans. In cryptography, plaintext is the input message that needs to be encrypted to ensure its confidentiality and security during transmission or storage. Once the plaintext is encrypted, it becomes ciphertext, which is not easily understandable to anyone without proper decryption keys or techniques. It is essential to secure the plaintext, especially when it contains sensitive or confidential information, such as passwords, financial data, personal information, and more.

c. Encryption Algorithm:

It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces cyphertext short, AES is a symmetric type of encryption, as it uses the same key to both encrypt and decrypt data. It also uses the SPN (substitution permutation network) algorithm, applying multiple rounds to encrypt data. These encryption rounds are the reason behind the impenetrability of AES, as there are far too many rounds to break through.

There are three lengths of AES encryption keys. Each key length has a different number of possible key combinations:

128-bit key length: 3.4 x 1038, **192-bit key length: 6.2 x 1057**, **256-bit key length: 1.1 x 1077**

Even though the key length of this encryption method varies, its block size - 128-bits (or sixteen bytes) - stays fixed.

The variety of key lengths poses some questions. Why are there multiple key lengths? And, if the 256-bit key is the strongest of the bunch (even referred to as “military-grade” encryption), why don’t we just always use it?

Well, it all comes down to resources. For example, an app that uses AES-256 instead of AES-128 might drain your phone battery a bit faster.

Luckily, current technology makes the resource difference so minuscule that there is simply no reason not to use 256-bit AES encryption.

d. Ciphertext:

It is the scrambled version of the plaintext produced by the encryption algorithm using a specific encryption key. The ciphertext is not guarded. It is on the public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

e. Decryption Method

It is a mathematical process, which produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext.

The decryption algorithm reverses the encryption algorithm and is thus closely related to it.

f. The Encryption Key

An encryption key is a sequence of bits or a string of characters that is used to encrypt or decrypt data in cryptography. Encryption keys can be of different lengths and types depending on the encryption algorithm used and the level of security required. In symmetric-key encryption, the same key is used for both encryption and decryption. In contrast, public-key encryption, which is also known as asymmetric-key encryption, uses a pair of keys - a public key and a private key - to encrypt and decrypt data.

The public key is used to encrypt the data, while the private key is used to decrypt the data. In either case, the strength of the encryption depends on the complexity and randomness of the key used.

g. Decryption Key

It is a value that is known to the receiver. The decryption key is related to the encryption key but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

h. Algorithm

An algorithm is a step-by-step procedure for solving a problem or accomplishing a task. It is a set of well-defined instructions that can be executed by a computer to perform a specific operation or solve a specific problem.

Algorithms are used in many different areas, including computer programming, data analysis, artificial intelligence, cryptography, and more. They are often expressed in pseudocode or programming languages and can range in complexity from simple to highly sophisticated. The efficiency and correctness of an algorithm are important considerations, and there are many different techniques and approaches that can be used to design and analyze algorithms.

COMMON ENCRYPTION ALGORITHMS

a. Data Encryption Standards

A symmetric-key approach for encrypting electronic data is called the Data Encryption Standard. Microsoft developed it in the early 1970s and it became a federal standard in the United States in 1977. DES encrypts and decrypts data in 64-bit blocks using a 56-bit key. Although DES was widely used for a long time, more modern encryption algorithms have subsequently replaced it because of its small key length, which left it open to brute-force attacks. The Advanced Encryption Standard has mostly replaced Data Encryption Standard.

b. RSA: Rivest, Shamir, and Adleman

RSA is a public key cryptographic algorithm named after its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. It is widely used for secure data transmission, digital signatures, and encryption. RSA involves generating a public key and a private key.

The public key is distributed to anyone who needs to send encrypted data to the owner of the private key, while the private key is kept secret and used to decrypt the data. The security of RSA is based on the difficulty of factoring the product of two large prime numbers, which is used to generate the keys. RSA is one of the most widely used and trusted encryption algorithms in the world.

c. Hashing

A hash function is a mathematical approach that takes any quantity of incoming information and produces a fixed-size output known as a hash value, message digest, or simply hash. The hash function is designed to be a straightforward-to-calculate but difficult-to-invert one-way function. Hashing is commonly used in computer security for a number of purposes such as data integrity, digital signatures, password storage, and message authentication codes.

Through the process of hashing, the original data is converted into a fixed-size digest. The digest is a unique representation of the original data, and even tiny changes in the information that was entered will result in an entirely new hash value.

This trait makes hashing valuable for confirming the accuracy of data because any changes to the data result in a different hash value, indicating that the data has been tampered with.

The original data cannot be recovered from the hash value since hashing algorithms are intended to be irreversible. As the original password is never stored, only its hash value, it is therefore practical for safeguarding sensitive data, such as passwords.

d. Message Digest Algorithm 5

The MD5 (Message Process Calculation 5) algorithm is a widely used cryptographic hash function that generates a fixed-length 128-bit hash value from an input message of arbitrary length. It was developed by Ron Rivest in 1991 to replace MD4 and has subsequently gained widespread adoption in numerous cryptographic applications, including automated marking and data integrity checks.

In any event, MD5 is no longer regarded secure for use in cryptographic applications since a number of flaws in the algorithm for computing have been discovered over time, including collisions (two distinct messages producing the same hash value), which could allow aggressors to develop sophisticated marks. and avoid using verification tools. Therefore, using SHA-2 or SHA-3 rather than MD5 is advised due to their higher level of security.

e. Standard for Advanced Encryption

Advanced Encryption Standard, which is NIST-approved (and employs the Rijndael block cipher).The National Institute of Standards and Technology, usually referred to as NIST, is a physical sciences research facility run by the US Department of Commerce. It functions as a non-regulatory body as well. To boost economic security and enhance the standard of life, the National Institute of Security develops and promotes technology, measurement, and standards. Numerous standards, including those relating to information security, cybersecurity, and cryptography, have been created with help from NIST. For example, NIST developed the NIST Cybersecurity Framework and the widely used AES encryption standard.

f. First Secure Hash Algorithm

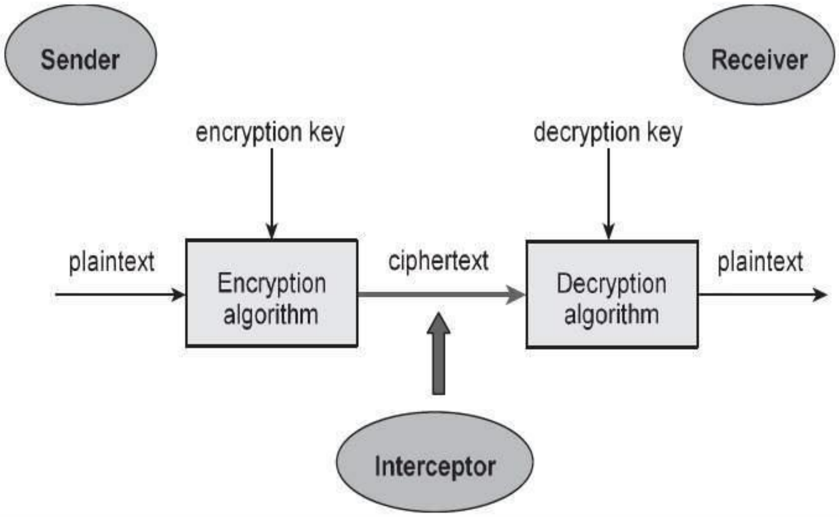
SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function developed by the National Security Agency (NSA) and released by the National Institute of Standards and Technology (NIST) in 1995. It generates a fixed-length, 160-bit (20-byte) hash value, often stated as a hexadecimal integer, which is used to validate digital data.

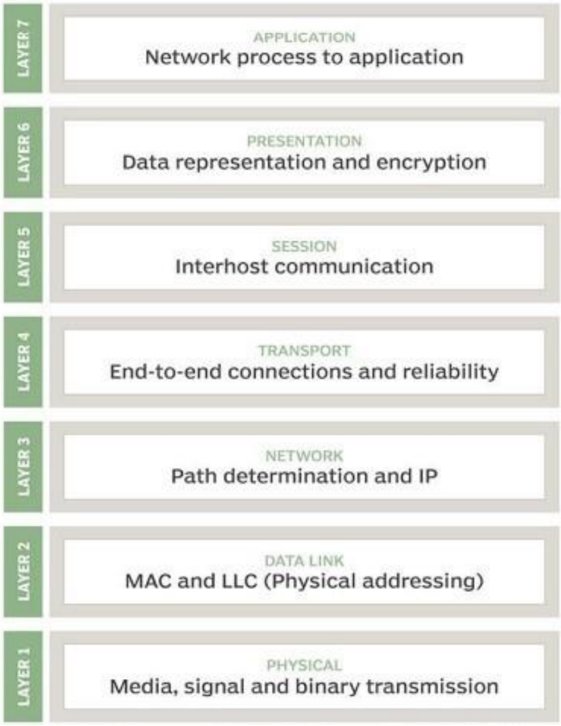
SHA-1 is no longer regarded secure for cryptographic uses due to multiple flaws discovered in its design, and it has been officially deprecated by NIST. Stronger hash algorithms like SHA-256 or SHA-3 are advised for usage in data integrity and authentication.
The likelihood of two separate messages having the same digest is decreased due to the big digest size.
message digest SHA-1. For this reason, SHA-1 is suggested as the preferred option.

g. The hash-based message authentication code

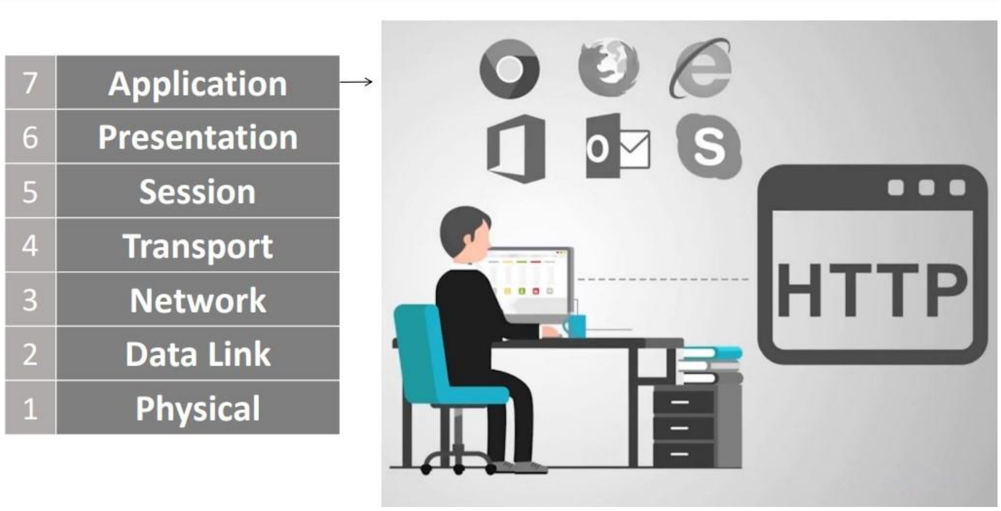
For messages that employ hashes, an authentication code. It is a cryptographic tool used to verify a message's accuracy and consistency. In along with a function called hashing, HMAC, which stands uses a confidentiality key that is shared by the person who sends it or the intended recipient.

(Anitha, January 2022)


Sender
Receiver
encryption key
decryption key
plaintext
Encryption algorithm
ciphertext
Decryption algorithm
plaintext
Interceptor

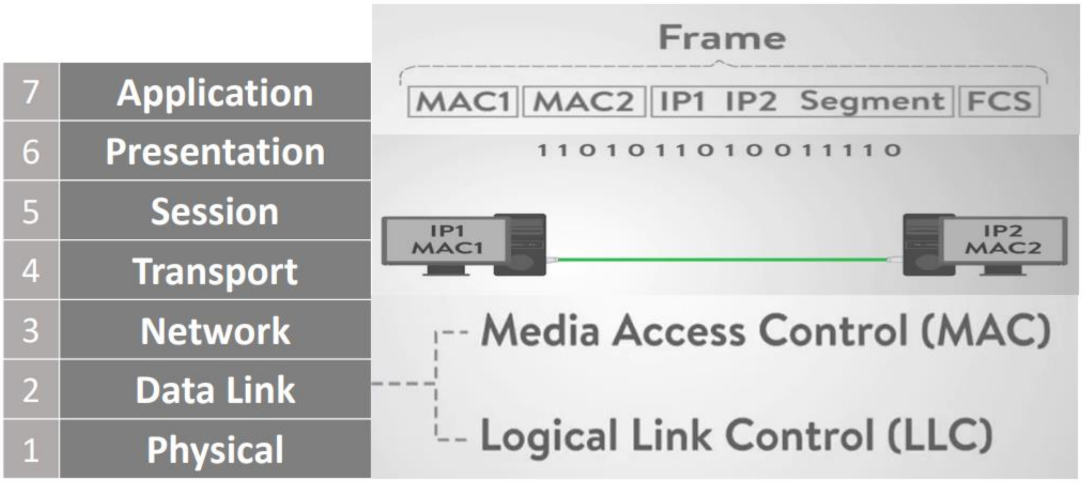

LAYER 7
APPLICATION
Network process to application
LAYER 6
PRESENTATION
Data representation and encryption
LAYER 5
SESSION
Interhost communication
LAYER 4
TRANSPORT
End-to-end connections and reliability
LAYER 3
NETWORK
Path determination and IP
LAYER 2
DATA LINK
MAC and LLC (Physical addressing)
LAYER 1
PHYSICAL
Media, signal and binary transmission

(Soltani, 24 December, 2020)



7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

(Soltani, 24 December, 2020)



(Soltani, 24 December, 2020)

REPEATED DENITION OF SERVICE

A distributed denial of service attack seeks to prohibit those with permission from visiting a web server. The main objective can be achieved in a number of ways, but they all center on utilizing the abilities of the server to the fullest. Memory, socket connections, CPU or database cycles, and network bandwidth are a few examples of these resources. Attackers might accomplish this through exploiting security holes in networks or standards, or they might just overtax the Web server by often using its capabilities.

Distributed denial of service attacks is simple and quick to execute since they don't depend on the Web application having a flaw or vulnerability. Using a server's weaknesses or vulnerabilities can but is not usually necessary for distributed denial of service attacks.
Each web server is only allowed to use a certain amount of CPU, memory, databases, and socket connections. The server won't have enough resources to handle legitimate requests from regular users if attackers send requests for features, they don't intend to utilize.

Because of this, authorized users can't access the website. The most startling aspect of these assaults is that they can penetrate even the most guarded servers. These attacks may be carried out via a variety of application-layer procedures, including HTTP, SOAP, DNS, and SIP. SIP and DNS use the connectionless UDP protocol, whereas HTTP and SOAP protocol use the connection-oriented communication protocol TCP as its foundation. assaults that take use of server characteristics may be divided into two categories: direct and reflected assaults. This class of assaults comes with a thorough nomenclature.

Attackers that use direct methods submit malicious queries to the victim server.
The server will crash if an attacker gives it a sufficient number many queries that it cannot handle. By generating such requests, the assailant must make a lot of effort by themselves during the process. These assaults are said to as symmetric. The attacker's goal is to take down a server using the least number of resources feasible. By deliberately constructing requests or providing a specific stream of requests in place of random ones, it is possible to make a server work harder. Such attacks increase the burden on the target server and lessen their impact on the attacker.

Symmetric DDoS attacks are similar to network layer DDoS assaults in many aspects. The similarity arises from the fact that, like network layer DDoS attacks, symmetric distributed interruption of service attacks function by barraging an intended Web server with a large number of attack requests, preventing it from responding to legitimate client requests.
However, distributed denial of service (DDoS) assaults at the application level utilizes HTTP, which stands for SOAP, DNS, or SIP while the network layer DDoS attacks use ICMP. Application-layer denial-of-service attacks are different from those at the network layer in that they sometimes may not require bandwidth restrictions on the server side to manifest. When compared to messages at the network's layer.

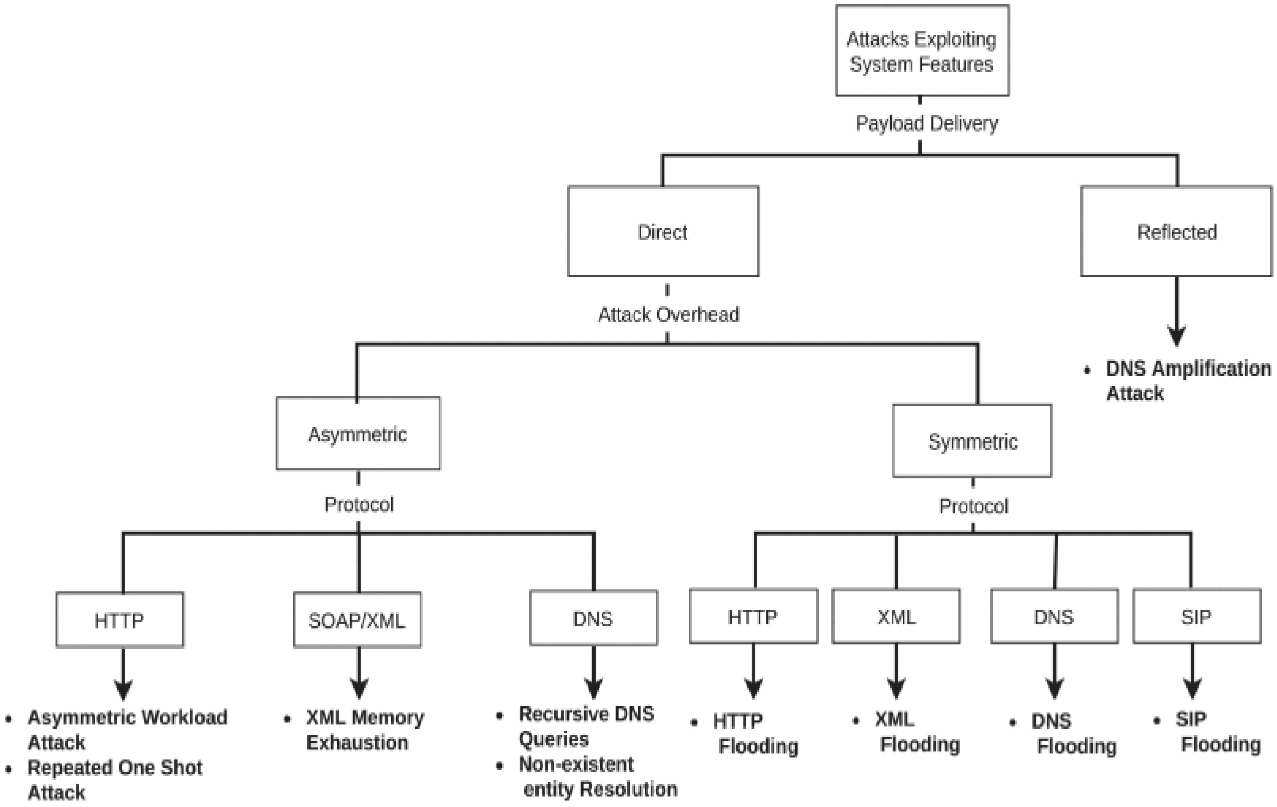


Fig3. Exploitation of Denial of service

HTTP flooding is the most common application layer DDoS attack using the HTTP protocol. This is mainly due to how easy the attack, etc., was to carry out.

This attack can only be carried out by sending several queries to a particular URL on the internet-based app that is being targeted. The hijacked pages are typically the login or home pages. Anyhow, a steady stream of reordered requests to the same URL can be quickly and effectively detected and rejected by the server chair. As a result, the next line of protection is to send queries to random URLs within the web application.

This attack functions similarly to the preceding one, except the consequence is unknown. It is trivial to deliver an HTTP surge with tools like the Moo Circle Particle Cannon (LOIC) or other push instruments for testing. The fact that these devices may be downloaded from the internet increases their hazard factor. SOAP or XML flood is similar to Https flooding in functioning, except it focuses on online services. The software layer's most crucial protocol is arguably DNS, which makes determining addresses easier. The header space is transformed into an internet protocol address (IP address) by an DNS provider in order to function. Ruth, the reality is that DNS uses the UDP protocol, rendering it vulnerable to assaults because anyone may instantly access the website's DNS. turn off the DNS.

After a period, the DNS server is unable to recognize unused queries and disconnects. This results in a much more serious issue than a web server being offline. If a web server fails, the organization will suffer.

When the DNS server fails, however, a substantial number of clients are disconnected from the majority of the web, because obtaining an IP address is a critical step in accessing any web service. Attacks on Dyn DNS happened in 2016. When the Dyn administration was deposed, many famous websites, including Twitter and Reddit, went offline for many hours. VoIP (Voice over Internet Protocol) is a modern kind of communication that offers manageability thanks to a phone exchange network that has been made available online.

Customers can now use VoIP as a mode of communication because of the lower cost of information. The Session Initiation Protocol is the most widely used VoIP convention. The caller, the registration center, the domain server, the proxy server, and the called party are all included in the technique. The caller and the called person are differentiated particularly by their IP and URL.

The registration server receives a call from a caller when it interacts with the arrangement. The client operators' zones, along with their IP addresses, are recorded by the region server. The call is transferred from the caller party to the called party through an intermediate server.

When the caller calls the called party, the caller sends a SIP INVITE message to the called party via an intermediary server. The intermediary server talks with the called party while also sending an Attempting message back to the calling party. When the called party receives the call, the phone begins to ring. Typically, a status message that says "RINGING" will indicate this. A 200 All message is sent by the phoned party when they accept the call.

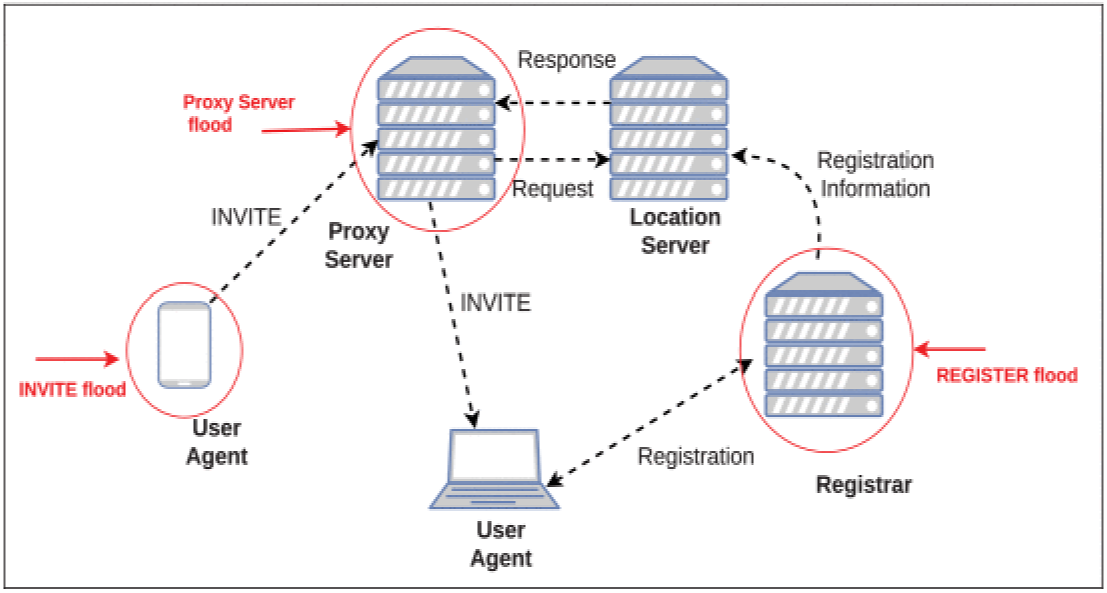


Fig3.Utilizing Protocol Features in Application Layer DDoS Attacks

SYMPTOMS OF DDoS ATTACKS

Denial of Service (DoS) assaults were among the first types of Web application threats. The first occurrence of what is now known as a DoS assault was documented in the late 1990s.
Since then, they have changed and become one of the most widespread attacks against Web applications. The amount many offenders taking part constitutes what differentiates a distributed denial of service assault from a Distributed Denial of Service attack. A DoS assault is frequently conducted by a small group of attackers, sometimes even just one. With hundreds or thousands of attackers, DDoS attacks are becoming more frequent.

These attackers do not have to be human, and in most cases, just a few human attackers are present. In this scenario, the "attackers" are computer programs operated by human attackers. Systems that have been infected with malware and are acting as attackers on behalf of the real attackers are referred to as zombies or bots. Attackers usually utilize a large number of these bots to form a botnet.

a. Slow network performance or unresponsiveness

Slow network performance or unresponsiveness is one of the most typical signs of a Distributed Denial of Service (DDoS) assault. This occurs when the attacker overloads the network, causing it to slow down or possibly become unresponsive.

This overwhelming traffic is sometimes referred to as a "flood" of traffic.
DDoS assaults may be extremely disruptive, causing major delays or preventing users from accessing websites or online services entirely. This may be particularly troublesome for firms that rely on their internet presence for day-to-day operations.
Network managers can utilize methods such as traffic filtering, rate restriction, and the deployment of content delivery networks (CDNs) to reduce the impact of DDoS assaults.

These methods can assist in detecting and blocking fraudulent traffic while allowing genuine traffic to flow through and maintaining network performance stability.
One of the most prevalent indications of a DDoS assault is this. The attacker's high bandwidth might cause the system in question to lag or possibly cease operation outright.

b. Increased spam emails

A DDoS attack can cause an increase in spam emails being sent from the network.
This is because the attacker may use compromised devices to send spam emails in addition to generating traffic to the targeted network or service. The spam emails may contain malware or phishing links, which can cause further harm to unsuspecting users who receive them. As a result, it is important to monitor email traffic and have proper email security measures in place to detect and block spam emails. DDoS attacks can also cause an increase in spam emails being sent from the network.

c. Unusual traffic patterns

Unusual traffic patterns are another symptom of a DDoS attack. These patterns may include spikes in traffic or traffic coming from unfamiliar sources. Normally, traffic on a network follows a certain pattern that can be easily predicted and managed by network administrators. However, during a DDoS attack, the traffic patterns become irregular, making it difficult for the network to manage the traffic flow and leading to slow network performance, unresponsiveness, and potentially even network outages. Network administrators may use traffic monitoring tools to detect unusual patterns and take action to prevent a DDoS attack from causing further harm to the network.

d. Inability to access websites.

DDoS assaults can prevent genuine users from accessing websites or internet services. The attack overwhelms the target server, rendering it unable to respond to genuine user requests.

As a result, the website or service may become unavailable, causing substantial disruptions to businesses and organizations that rely on their online presence. Users that attempt to access the website or service may receive error messages or timeouts.

A DDoS assault can also make it impossible for people to access websites or online services.

e. Increased latency

Increased latency refers to the delay in data transmission between two points on a network. In the context of a DDoS attack, increased latency can occur because of the excessive traffic generated by the attacker. As a result, data packets take longer to reach their destination, and the network may become slow or unresponsive. This can result in delays, slow performance, and other issues that can impact the usability of the network. Increased latency is a common symptom of a DDoS attack and can indicate that there is an ongoing attack that needs to be addressed.

f. Outages

DDoS attacks can cause outages in critical services, such as online banking, e-commerce, or government websites. This can result in a loss of revenue, damage to reputation, and even impact on public safety if critical services such as emergency services are affected. Outages can last for varying amounts of time, depending on the severity of the attack and the effectiveness of the mitigation measures in place.

g. Network congestion

Network congestion is a symptom of a DDoS attack, where the excessive traffic generated by the attacker causes a bottleneck in the network. This can slow down the network and prevent users from accessing critical services, such as online banking, e-commerce, or government websites. Congestion can occur at various points in the network, such as routers, switches, or firewalls, and can result in delays, slow performance, or even outages. To mitigate network congestion caused by a DDoS attack, network administrators can use traffic filtering, load balancing, or other techniques to manage the traffic and prevent it from overwhelming the network.

HOW DOES DISTRIBUTED DENIAL OF SERVICE WORKS

A DDoS (Distributed Denial of Service) attack works by overwhelming a targeted server or A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Several compromised computer systems are used as sources of attack traffic in DDoS attacks to achieve efficacy. Computers and other networked resources, such as IoT devices, are examples of exploited machinery.
DDoS assaults are conducted using networks of computers linked to the Internet.
These networks are made up of computers and other devices, such as Internet of Things (IoT) devices, that have been infected with malware, enabling a hacker to remotely manage them. These particular gadgets are known as bots (or zombies), and a botnet is a collection of bots.

Once a botnet has been built, the attacker can conduct an attack via remote instructions to each bot.
When a victim's server or network is targeted by the botnet, each bot sends queries to the target's IP address, potentially overloading the server or network and resulting in a denial-of-service to regular traffic.
Separating attack traffic from regular traffic can be challenging because each bot is a valid Internet device.

.

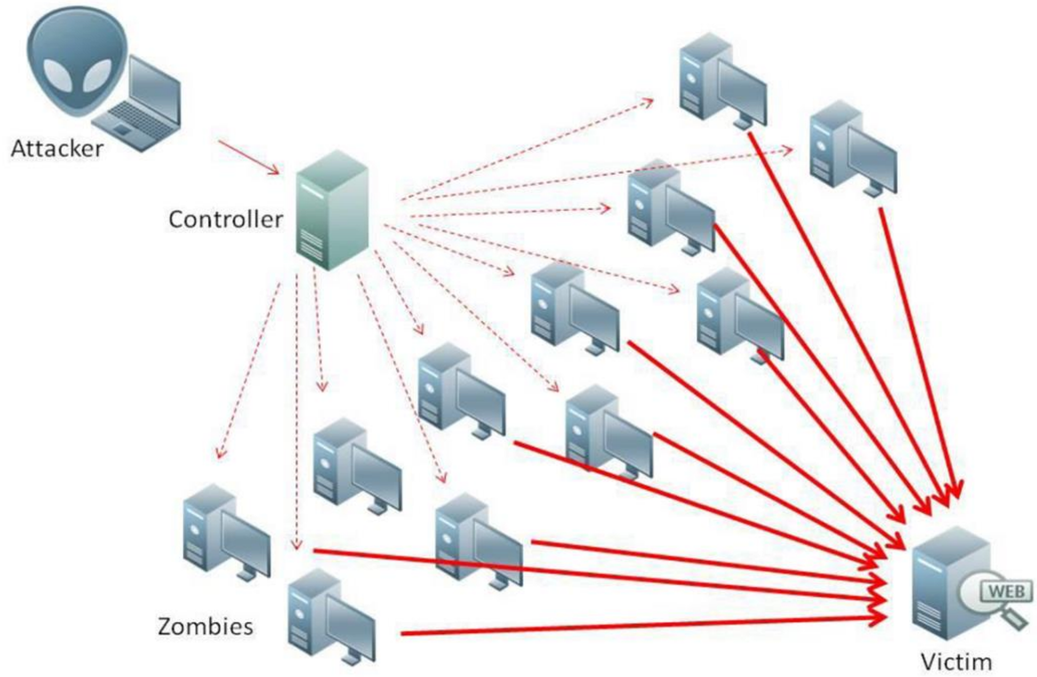


Fig 3. DDoS Cloudflare

DDoS ATTEMPTS: TYPES

Different DDoS attacks focus on various network connection components. To understand how various DDoS attacks work, it is necessary to first understand how a network connection is established.

On the Internet, a network link is made up of various parts or "layers." In the same way that a house is built from the ground up, each layer in the model serves a certain function.

The OSI model, which is shown in the illustration below, is a conceptual framework for representing connections to networks at seven different layers.

a. Volume attacks

Volume attacks are a type of DDoS attack that overwhelms a targeted network or system with a massive amount of traffic, making it difficult or impossible for legitimate traffic to pass through. These attacks are typically conducted using a botnet, which is a group of compromised devices that are controlled by an attacker.

In a volume attack, the botnet sends a flood of traffic to the target, saturating its bandwidth and causing it to become unresponsive. The traffic can come in different forms, such as TCP, UDP, ICMP, or HTTP requests. The attack traffic can also be amplified using techniques such as IP spoofing or DNS amplification, which can increase the volume of traffic sent to the target.

Volume attacks can also take advantage of vulnerabilities in the target system to further amplify the attack. For example, a UDP amplification attack can exploit a vulnerability in certain UDP-based protocols to increase the volume of traffic sent to the target.

Overall, volume attacks are a common type of DDoS attack that can be difficult to defend against due to their massive scale and the use of sophisticated techniques to amplify the attack traffic.

b. TCP State-Exhaustion attacks

TCP State-Exhaustion attacks are a type of DDoS attack that exploits the stateful nature of the Transmission Control Protocol (TCP) to consume the resources of a target system. In a TCP State-Exhaustion attack, the attacker floods the target system with a large number of TCP connection requests, overwhelming the system's ability to manage them and causing it to crash or become unresponsive.

TCP is a connection-oriented protocol that uses a three-way handshake to establish and maintain a connection between two systems. During the handshake, the client sends a SYN packet to the server, the server responds with a SYN-ACK packet, and the client completes the connection by sending an ACK packet. This process creates a stateful connection between the two systems, which requires the system to maintain information about each connection.

TCP State-Exhaustion attacks can be especially effective because they can be launched using low-bandwidth connections, making them difficult to detect and mitigate. Additionally, many network devices and applications are vulnerable to TCP State-Exhaustion attacks because they have limited resources for handling TCP connections. To protect against TCP State-Exhaustion attacks, network administrators can use techniques such as rate limiting, traffic filtering, and deploying specialized hardware and software solutions designed to detect and mitigate DDoS attacks.

c. Application Layer attacks

Application Layer attacks, also known as Layer 7 attacks, target the application layer of network stack, which is responsible for providing services to end-users. These attacks are often more difficult to detect and mitigate than other types of DDoS attacks because they are legitimate requests from the user, making them hard to distinguish from legitimate traffic.

d. HTTP Flood

This type of attack targets web servers and applications by flooding them with HTTP requests, making them unavailable to users.

e. DNS Flood

In this type of attack, the attacker sends a large number of DNS requests to a server, overwhelming it and making it unable to respond to legitimate requests.

f. DDoS Botnet

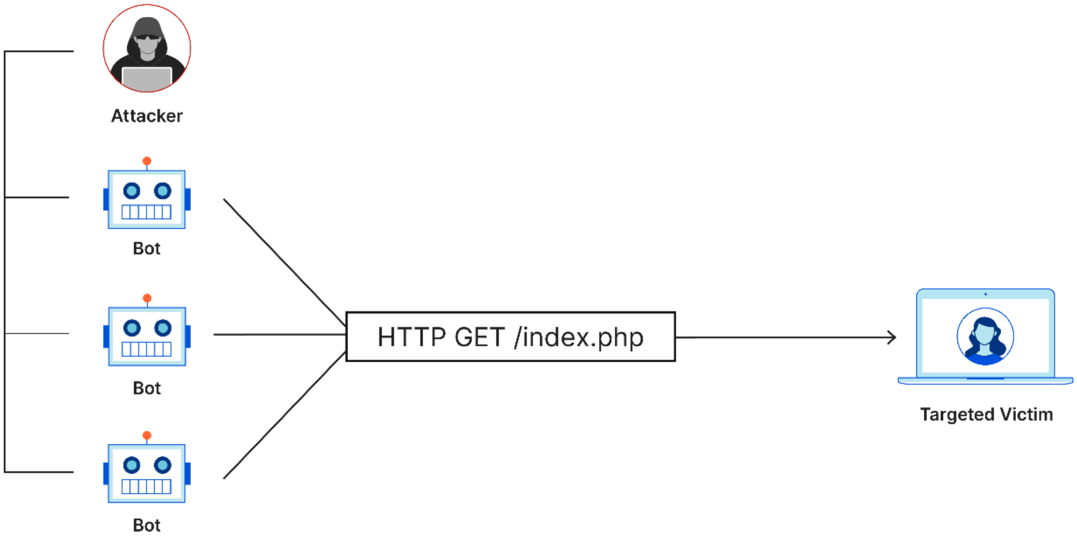
A botnet is a network of hacked devices that the attacker commands to perform a coordinated attack on a target. Bot networks can be used to carry out Application Layer assaults.

g. Application-layer protocol attacks

These attacks target specific protocols such as HTTP, SMTP, or SIP by exploiting vulnerabilities in the protocol implementation.

h. Protocol attacks

Protocol assaults are a sort of DDoS attack that target weaknesses in network protocols, such as the TCP/IP protocol stack. These attacks take use of flaws in network protocols' traffic management, resulting in network congestion, device failures, or other service interruptions.
The Ping of Death attack, which delivers massive packets of data to a target device to make it crash or go unresponsive, is an illustration of a protocol attack.


Attacker
Bot
Bot
Bot
HTTP GET /index.php
Targeted Victim

TRANSPORT LAYER

SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a protocol used to establish an encrypted link between a web server and a client (such as a web browser). Encrypted attacks are DDoS attacks that utilize SSL/TLS encryption to mask malicious traffic and make it more difficult for network defenses to detect and mitigate the attack.

SSL/TLS attacks can take several forms, including:

a. SSL/TLS Flood

SSL/TLS flood is a type of DDoS attack that targets the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols used to encrypt web traffic. The attack floods the server with a large number of SSL/TLS connection requests, overwhelming its processing power and causing it to become unresponsive.

The SSL/TLS flood attack can be launched from a single or multiple source IP addresses, and it can target specific SSL/TLS ports or use random ports to evade detection. The attack can also use fake SSL/TLS certificates to bypass the server's security measures.

To prevent SSL/TLS flood attacks, organizations can implement network-level protections such as firewalls, load balancers, and intrusion prevention systems.

They can also use SSL/TLS offloading to reduce the load on the server and distribute the traffic across multiple servers.

b. SSL/TLS renegotiation attack

This attack exploits a vulnerability in SSL/TLS protocol that allows an attacker to repeatedly renegotiate a connection with a server, creating a high CPU load on the server and causing it to become unresponsive.

c. SSL/TLS handshake attack

An SSL/TLS handshake attack is a type of cyber-attack that targets the handshake process of the SSL/TLS protocol, which is used to establish a secure communication channel between a client and a server over the internet. The handshake process involves a series of steps, including authentication and key exchange, to ensure the confidentiality and integrity of the communication. In an SSL/TLS handshake attack, the attacker exploits vulnerabilities in the handshake process to disrupt the communication or steal sensitive information.

One common type of SSL/TLS handshake attack is the man-in-the-middle (MITM) attack, where the attacker intercepts the communication between the client and server and poses as the server to obtain the client's credentials or other sensitive information.

Another type of SSL/TLS handshake attack is the SSL/TLS renegotiation attack, where the attacker initiates a renegotiation of the SSL/TLS connection to consume server resources or cause a denial-of-service (DoS) attack. This type of attack can be prevented by disabling SSL/TLS renegotiation or implementing rate limiting and monitoring mechanisms.

To protect against SSL/TLS handshake attacks, it is important to use strong encryption and authentication protocols, regularly update the SSL/TLS implementation, and monitor for abnormal traffic patterns or suspicious activity.

d. Encrypted DDoS attacks

This kind of attack uses SSL/TLS encryption to disguise malicious traffic and make it more challenging for network defenses to identify and neutralize the assault. Several attack types, including volumetric assaults, application layer attacks, and TCP state-exhaustion attacks, can fall under this category.

Distributed denial of service attacks aims to deplete the resources of the victim.

These resources may include computational power, network bandwidth, or operating system data structures.

Malicious users first set up a network of machines on which they would rely to generate the amount of traffic required to prevent computer users from using services. Attackers identify weak hosts or websites on the network and then construct an attack network using those findings. Typically, vulnerable hosts are those that are not properly patched, are not running any antivirus software, are running outdated antivirus software, or are both. Attackers then employ vulnerable hosts as a means of access by utilizing their weakness. The intruder's subsequent move is to set up new software applications.

TYPES OF DDoS ATTACKS

Single IP single port

A single IP single port DDoS assault is a kind of distributed denial of service assault that occurs when a lot of requests are delivered to a single IP address and port from several sources, saturating the targeted system with traffic and rendering it inaccessible.

As it seeks to overwhelm the target with a lot of traffic, this kind of assault is sometimes referred to as a volumetric attack.

Attackers frequently make use with a botnet, which are distributed networks of hacked devices that can be remotely controlled, to carry out single Internet Protocol (IP ports denial of service (DDoS) attacks. The botnet is used to flood the target IP address and port with connections in a conscious choice to eliminate its resources and block genuine users from accessing it.

There are various techniques that can be used to mitigate single IP single port DDoS attacks, including rate limiting, filtering, and block-listing. Rate limiting involves setting a limit on the number of requests that can be received from a single IP address, while filtering involves identifying and blocking traffic from known malicious IP addresses.

Block-listing involves maintaining a list of IP addresses that have been identified as sources of DDoS attacks and blocking all traffic from those addresses.

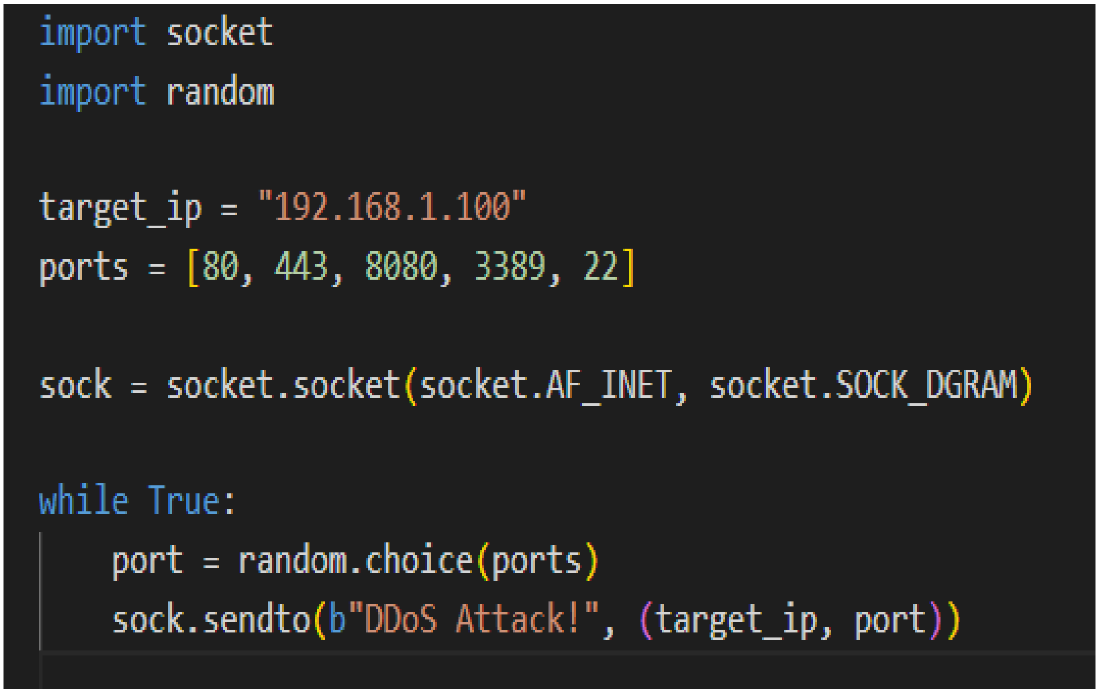
Single IP multiple port

A single IP multiple port DDoS attack is a type of DDoS attack that involves overwhelming a target system by flooding it with traffic from a single IP address across multiple ports. In this type of attack, the attacker sends a large number of requests to the target system from a single IP address, but each request is directed at a different port on the target system.

The target system then has to process each request and respond accordingly, leading to a significant increase in traffic and resource consumption. This type of attack is difficult to detect and mitigate because it is legitimate traffic from a single IP address.

Single IP multiple port attacks can be launched using a variety of techniques, such as using a botnet to distribute the attack traffic or using a reflection or amplification attack to increase the volume of traffic being sent to the target system.

These attacks can be used to target a variety of systems, including web servers, email servers, and DNS servers.



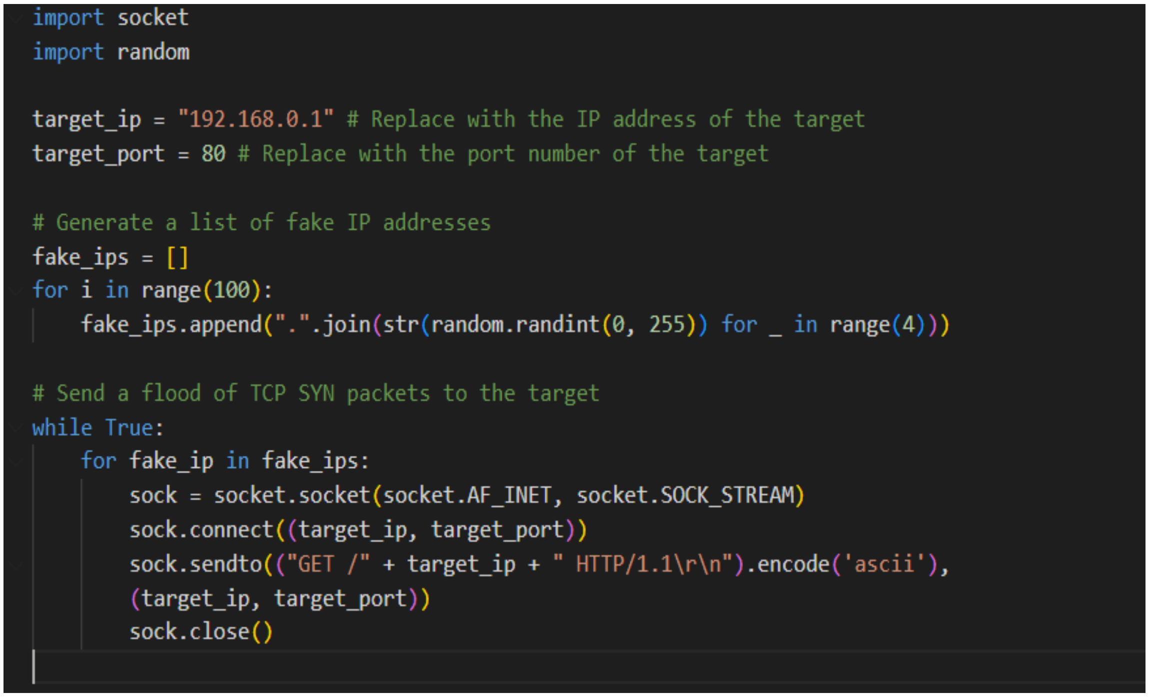
```python
import socket
import random

target_ip = "192.168.1.100"
ports = [80, 443, 8080, 3389, 22]

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

while True:
    port = random.choice(ports)
    sock.sendto(b"DDoS Attack!", (target_ip, port))
```

e. Multiple IP single port

In a Multiple IP single port DDoS attack, the attacker uses multiple compromised devices (often called a botnet) to flood the target network with a high volume of traffic on a single port, overwhelming the target system's ability to respond to legitimate requests.
This type of attack is particularly effective against systems with limited resources that are not capable of handling large amounts of traffic. It can also be used to target specific services, such as HTTP (port 80) or Domain Name System (DNS - port 53).

One example of this type of attack is the Mirai botnet, which used a large number of compromised Internet of Things (IoT) devices to launch a massive DDoS attack against DNS provider Dyn in 2016, causing widespread disruption to popular websites and online services. To implement this type of attack in Python, the following code can be used.

This code creates a list of 100 fake IP addresses and sends TCP SYN packets to the target IP address on the specified port, using each of the fake IP addresses.
This can result in the targeted server or network becoming overwhelmed with traffic and unable to respond to legitimate requests.



```python
import socket
import random

target_ip = "192.168.0.1" # Replace with the IP address of the target
target_port = 80 # Replace with the port number of the target

# Generate a list of fake IP addresses
fake_ips = []
for i in range(100):
    fake_ips.append(".".join(str(random.randint(0, 255)) for _ in range(4)))

# Send a flood of TCP SYN packets to the target
while True:
    for fake_ip in fake_ips:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.connect((target_ip, target_port))
        sock.sendto(("GET /" + target_ip + " HTTP/1.1\r\n").encode('ascii'),
        (target_ip, target_port))
        sock.close()
```

SCOPES AND OBJECTIVES

Things that are safe, secret, cryptic, and obscured are represented by cryptography. A numerical method for securely delivering intimate girlfriend messages across doubtful routes is encryption. Encryption has been used for nearly 2000 years as a fundamental method of safeguarding sensitive information against many forms of attackers, including impedance, tampering, and tampering.

They tattooed words on and grew down the locks from their slaves' heads. Cryptography's primary application dates back to 1900 BC. when Egyptian copyists infused their etchings with intriguing meanings. According to some specialists, ranging ciphers first appeared soon after manuscripts were written and were used for everything from combat plans for war to reconciling messages. The Caesars Code

Each character in the character set is shifted by the provided number of positions. It is brittle. As a generalization of Caesar's motion cipher, Vigenère's polyalphabetic cipher uses all letters. It takes a slogan to choose a scrambling route. 26-character level with word references, substitution cipher. It is brittle. Various cryptographic computations are now carried out within the specified date as explained in the remaining sections of this chapter. Most modern cryptographic computations are based on the fundamental method of computing extended integrability to prime numbers, which is said to be difficult. In both symmetric and divergent cryptosystems, encryption is the process of transforming the dominant form of some substance into a complex form, while decryption extracts the dominant form of data from unrelated substances. Secondary encryption uses plaintext and source code for analysis, keeping an important distance from data development.

The motive of encryption is to ensure total confidentiality, verification, and validity of information. Encryption is a method of secure communication used to achieve these goals by converting plaintext (clear data) into ciphertext (unintelligible data) that can be viewed, so to speak, by the intended recipient. increase. Keep it a secret. The main purpose of encryption is to ensure the protection of information.

This is usually routinely done by encrypting the information so that it cannot be viewed by unauthorized persons. Encryption is the conversion of plaintext into ciphertext using an encryption method and a puzzle key. The ciphertext can be decrypted (converted to plaintext) by someone who has the puzzle key.

This means that there is a guarantee that the information has not been altered or adapted in any way. This can be accomplished by using message authentication codes (MAC) or extended signatures. A MAC is a code created by cryptographic computation and a secret key and is used to ensure that messages have not been altered in transit. A computer signature is a code created by cryptographic computation and a private key, used to verify that a message was sent by the person claiming to be the sender.

Authenticity

The authenticity of the data is further ensured via cryptography. This suggests that it ensures the information is from the source it claims to be. An advanced certificate or an open key foundation (PKI) are typically used to complete the process.

An advanced certificate is a digital record that certifies the sender's identity and personality.

A PKI could be a system that encrypts communication and verifies the sender's identity using digital certificates.

In rundown, the most targets of cryptography are to ensure the secrecy, judgment, and genuineness of data. It is utilized to secure touchy data from unauthorized get to, guarantee that the data has not been altered with, and guarantee that the information is from the source it claims to be from.

The secure trade of key among sender and beneficiary may be a parcel of inconvenience a few errands in as set basic sensor arrange. information need to be mixed to begin with by clients some time recently it is outsourced to a inaccessible dispersed capacity advantage and both data security and data get to security have to be guaranteed to such an degree that disseminated capacity master organizations have no capacities to unscramble the data, and when the client has to interest a number of segments of the whole data, the conveyed capacity system will allow the accessibility without recognizing what the fragment of the encoded data came back to the client is around.

Integrity

Keenness in cyber security alludes to the strategies of guaranteeing that information is exact, genuine, and defended from unapproved user modification or devastation. Information judgment moreover alludes to the precision and legitimacy of information over its whole lifecycle. After all, compromised information is of small or no intrigued to associations of any measure, not to specify the included dangers that come with sensitive information misfortune.

A keenness in cyber security illustration can incorporate when data comprises data that's transmitted between frameworks and/or when put away on frameworks, such as email. In this manner, keeping up information keenness is a key portion of most undertaking security arrangements nowadays.

This principle will be advanced investigated afterward on inside this article.

Keeping up astuteness isn't as if it were vital to control get to at a framework level, but to guarantee that clients can as it were change data that they are approved to modify.

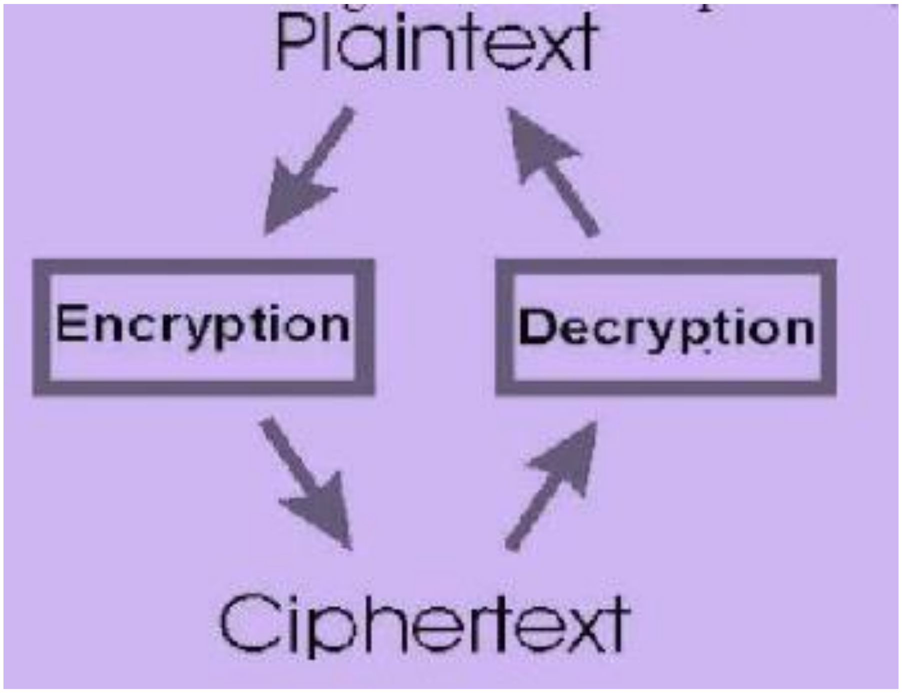
When looking at the best ways to protect your touchy data, integrity in cyber security is the key step to guaranteeing that your organization secures its resources.

Information keenness is greatly critical in cybersecurity since it traces three fundamental objectives that ought to be followed to by cybersecurity groups:

Anticipating unapproved clients from making modifications to programs or information.

Anticipating approved clients from making unapproved or dishonorable alterations.

Keeping up both the inner and external consistency of programs and information.



(Salah, October 2020), (W. Stallings, 2019), (Anitha, January 2022)

FUCNTIONALITY OF ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard is a symmetric encryption algorithm that encrypts data using block ciphers. Designed to be safe, fast, and efficient. Advanced Encryption Standard is a symmetric encryption that has been chosen by a number of government organizations, including the US government, to safeguard confidential data. Advanced Encryption Standards are used for protecting confidential information in software and hardware all over the world. This is essential for government computer security, cyber security, and electronic privacy.

Key Expansion

Key expansion is the process of the AES encryption algorithm that expands the original key into a larger set of subkeys that are used during the encryption and decryption process. The key expansion process involves multiple steps such as permutation, permutation, and merging operations that transform the original key into a set of round keys used in each round of the AES encryption process. Key expansion first splits the original key into multiple 32-bit words. These words are used to generate additional words using a series of permutation, shift, and shuffle operations. The specific operations used in key expansion depend on the size of the key, with larger key sizes requiring more rounds of expansion.

For example, in AES-128, the original key is expanded into a set of 44 words, each word 32 bits long. The key expansion process for AES-128 involves four rounds of key expansion, with each round applying a series of permutation, shift, and shuffle operations to the words generated in the previous round. Once the key expansion process is complete, the resulting set of round keys is used during the encryption and decryption process. Each round of encryption or decryption uses a different round key, and the final round key is used to transform the ciphertext or plaintext into the final output. key being used to transform the ciphertext or plaintext into the final output.

Initial Round

The first round of the AES method involves XORing the plaintext with the first-round key. This is where the process of transforming unencrypted to cipher text begins. This XOR method generates a byte matrix known as the state matrix.

The state matrix is then processed using several rounds, each of which includes the four operations Sub-Bytes, Shift Rows, Mix Columns, and AddRoundKey. The number of rounds varies according to the key length, with 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key.

In the Sub Bytes stage, each byte in the state matrix is replaced with a corresponding byte from the AES S-box. Using a 256-bit fixed table called the S-box, to conduct nonlinear substitutions on each byte of the state matrix.

The bytes in each row of the state matrix are shifted to the left by a given number of bytes in the Shift Rows step. The number of rows dictates how many bytes are moved, with the first row remaining unchanged and the last row shifting by three bytes. The Mix Columns step multiplies each column of the state matrix by a fixed matrix of four bytes to create a new column.

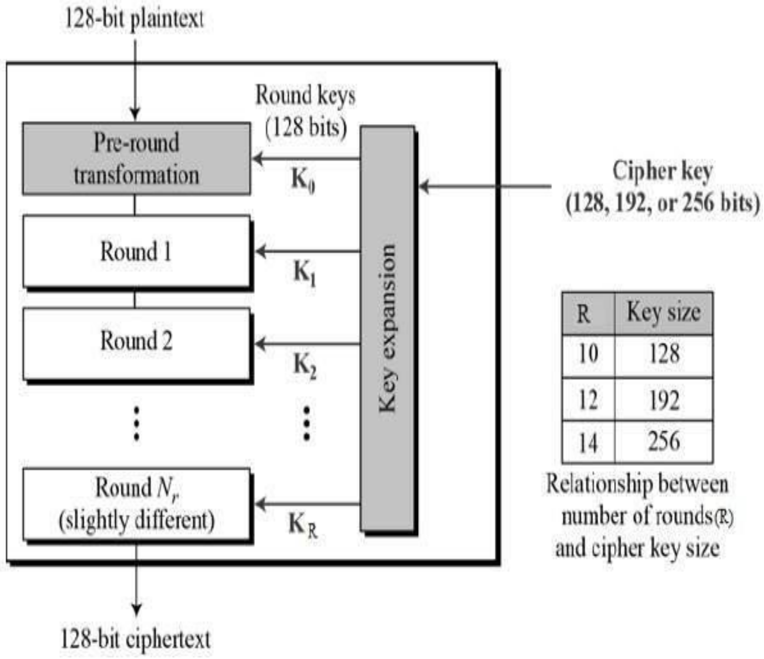
This step provides diffusion across columns and increases the complexity of the encryption. Finally, in the AddRoundKey step, the state matrix is XORed with a round key that has been generated from the original encryption key using the Key Expansion process. This step provides confusion across the rows and ensures that each round key is unique. After the final round, the resulting state matrix is the ciphertext that corresponds to the original plaintext.

Rounds

AES performs a series of rounds (10, 12, or 14, depending on the key size), each consisting of four distinct operations: Sub Bytes, Shift Rows, Mix Columns, and AddRoundKey. These operations combine to produce a highly secure and efficient encryption process.

Final Round

The Mix Columns procedure is skipped in the final round of AES to simplify the decryption process. AES decryption is the opposite of encryption in this operation. The round keys are utilized in reverse order, and each round action is carried out in the opposite direction.



R	Key size
10	128
12	192
14	256

Relationship between
number of rounds(R)
and cipher key size

THEORETICAL RESULT OF CRYPTOGRAPHY AND NETWORK SECURITY

Encryption encrypts messages so that only authorized users may decrypt them using algorithms and protocols. Encryption converts plain text into ciphertext by using an encryption algorithm and a secret key. The ciphertext can then be safely transmitted over the network or stored in a secure location. The private key is required by the recipient in order to decrypt the ciphertext.
The encryption can be broken, and the original plaintext can be retrieved using the private key. Digital signatures, which can be used to confirm the legitimacy of online data or communications, are also created using encryption.
A digital signature is generated through encapsulating a fixed-length message corresponding to the document that was originally signed with the signer's secret key.

The created digital signature can be delivered together with the document or message, and the recipient can validate it using the signer's public key. Cybersecurity encompasses preventing unauthorized access, use, disclosure, damage, alteration, or destruction of network computers and the components that make them up (hardware, software, data, etc.). Firewalls, intrusion detection systems, virtual private networks (VPNs), access control systems, and encryption are some examples of cybersecurity methods.

Firewalls are used to limit the accessibility of networks by filtering incoming and outgoing traffic using specified rules.
Unauthorized access attempts and other suspicious activities on the network are found using intrusion detection systems, which notify administrators of the situation. Secure remote access to your network via the Internet is made possible by VPNs.

Access control systems are used to limit user permissions and prevent unwanted access to sensitive data. Even in the presence of adversaries, they make it convenient to communicate securely and reliably. To secure the confidentiality, integrity, and availability of data and communications in today's networked world, effective use of encryption and security precautions remains crucial.

RECOMMENDATIONS

Recommendations for encryption and network security in order to give the appropriate level of protection, encryption must be properly applied, which is a crucial component of information security.

Here are some encryption suggestions.
Use strong encryption algorithms that are currently regarded as secure and that have not been compromised. AES-256 is now regarded as one of the most secure encryption algorithms available and should be utilized whenever possible.

Proper key management is required to keep encryption keys safe and secure from unauthorized access. It is important to give considerable thought to key length, complexity, and rotation time.
When exchanging encryption keys, it is important to use secure methods that prevent unauthorized access. To ensure that keys are exchanged securely, key exchanges should use public key cryptography, such as RSA.

Maintain regular software updates. Software for encryption should be updated frequently to guarantee that security flaws are corrected.

Prevent side-channel assaults. Side-channel attacks target flaws in cryptography's physical implementation, such as power usage and electromagnetic radiation. Use defense strategies like masking and blinding to fend offside-channel attacks.

Follow industry best practices to ensure that your encryption is correctly implemented, as published by the National Institute of Standards and Technology. regular security inspections Regular security audits should be undertaken to ensure that encryption is correctly applied and that no vulnerabilities exist.

IMPLICATIONS OF THEORY AND PRACTICE

Theories and practices in the field of cryptography and network security have significant implications for research. They provide a foundation for understanding the underlying principles and concepts that govern the field and guide research efforts.

Implications of theory and practice in research related to cryptography and network security:

a. **Framework for Research**

Theories and practices provide a framework for research in cryptography and network security. Researchers can use these frameworks to formulate research questions, design experiments, and analyze results.

b. **Evaluation of Existing Methods**

Theories and practices can be used to evaluate the effectiveness of existing methods. Researchers can use these frameworks to assess the security and reliability of existing encryption algorithms, intrusion detection systems, and access control mechanisms.

c. **Identification of Research Gaps**

Theories and practices can assist in identifying research gaps. These frameworks allow researchers to pinpoint areas that still require study in order to increase the security and dependability of network systems.

d. **Development of New Methods**

Theories and practices can be used to develop new methods for cryptography and network security. Researchers can use these frameworks to design new encryption algorithms, intrusion detection systems, and access control mechanisms that are more secure and reliable than existing methods.

e. **Standardization of Methods**

Theories and practices can be used to standardize methods in cryptography and network security. Standardization is essential to ensure interoperability and compatibility between different systems and applications.

APPENDIX A

This appendix contains additional information and resources on cryptography and network security that I discovered while conducting online research. The knowledge provided here is meant to complement my primary work and provide readers a more thorough understanding of this particular subject.

The study of secure communication methods in the presence of outside parties is known as cryptography. To prevent illegal access and interception, it uses a variety of encryption techniques. Cryptography is frequently used to safeguard sensitive data, such as personal information, financial data, and study findings, during my in-person and online research.

Network security refers to the measures taken to protect a computer network from unauthorized access, cyber-attacks, and other security threats. Network security is a critical concern in our everyday life activities, as the internet is a common target for hackers and cybercriminals.

Cryptographic technique consists of the following listed below and its importance.
Symmetric key cryptography: This involves using the same key to encrypt and decrypt data. The key must be kept secret to ensure the security of the data.

Asymmetric key cryptography: This involves using a pair of keys – a public key and a private key to encrypt and decrypt data. The public key is made available to anyone who wants to send encrypted data, while the private key is kept secret by the recipient.

Hash functions: These are mathematical functions that can be used to transform data into a fixed-length string of characters. Hash functions are often used to verify the integrity of data, as any changes to the original data will result in a different hash value.

Resources for Cryptography and Network Security in Online Research

There are several resources available to researchers who need to implement cryptography and network security measures in their online research projects.

The National Institute of Standards and Technology (NIST) provides guidelines and standards for cryptographic techniques and network security.

The International Association for Cryptologic Research (IACR) is a professional organization that promotes research in cryptography and related fields.

The Electronic Frontier Foundation (EFF) is a nonprofit organization that advocates for online privacy and security.

The Open Web Application Security Project (OWASP) provides resources and guidelines for secure web application development.

The Center for Internet Security (CIS) provides guidelines and best practices for securing computer networks.

References

Anitha, S. (January 2022). A Study on Network Security and Cryptography. *AICTE CONFERENCE* (pp. 1-8). Tamil Nadu, ResearchGate.

Damico, T. M. (2009). A Brief History of Cryptography. *Student Pulse*, 1(11).

J, A. (22 May 2015). Network Security and Types of Attacks in Network. *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015). 48*, pp. 503-506. Bhubaneswar, Odisha, India: Elsevier. doi:10.10.16

Mohan, P. V., & J, A. (2015). Types of Attacks in Network Security. *Procedia Computer Science*, 1.

Praseed, A., & Thilagam, P. (2019). Development of Tools for Detection of Application Layer DDoS Attacks on Web Applications. *IEEE Communications Surveys & Tutorials. 21*, pp. 661 - 685. Surathkal, India: IEEE.

Rogaway, P. (2004). Nonce-Based Symmetric Encryption. In P. Rogaway (Ed.), *Conference on Computer and Communications Security (CCS 2002). LNCS,volume 3017*, p. 1. New York : springer. doi:10.1007/978-3-540-25937-4_22

Salah, K. (October 2020). New Frontiers in Cryptography. *Confidentiality*, 1. Retrieved from http://dx.doi.org/10.1007/978-3-030-58996-7_2.

Selvam, A. (January 2022). A Study on Network Security and Cryptography. *AICTE CONFERENCE* (pp. 1-8). India: ResaerchGate.

Soltani, D. (24 December, 2020). Network security in OSI model. *OSI,security,threat,risk,capabilities*, 66.

W. Stallings, L. B. (2019). Computer Security. *Principles and Practice (Pearson, Harlow)*, 1.

WANG, LINGYU; SINGHAL, ANOOP; Jajodia, Sushil ; Noel, Steven. (1, July 2010.). Measuring Security Risk of Networks Using Attack Graphs. *International Journal of Next-Generation Computing. 1*, pp. 1-13. Quebec: researchgate. Retrieved 05 6, 2023

(Kanber et al. 2022)