Sarvasiddhant Education Society's
SWAMINARAYAN SIDDHANTA INSTITUTE OF TECHNOLOGY
Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University
Nagpur Katol Highway Road, Khapri (Kothe),
Tal.Kalmeshwar, Nagpur, Maharashtra 441501
Department Of Computer Engineering
Session 2023-2024

CNS NOTES

CRYPTOGRAPHY & NETWORK SECURITY

SEMESTER: 7TH SEM (FINAL YEAR)

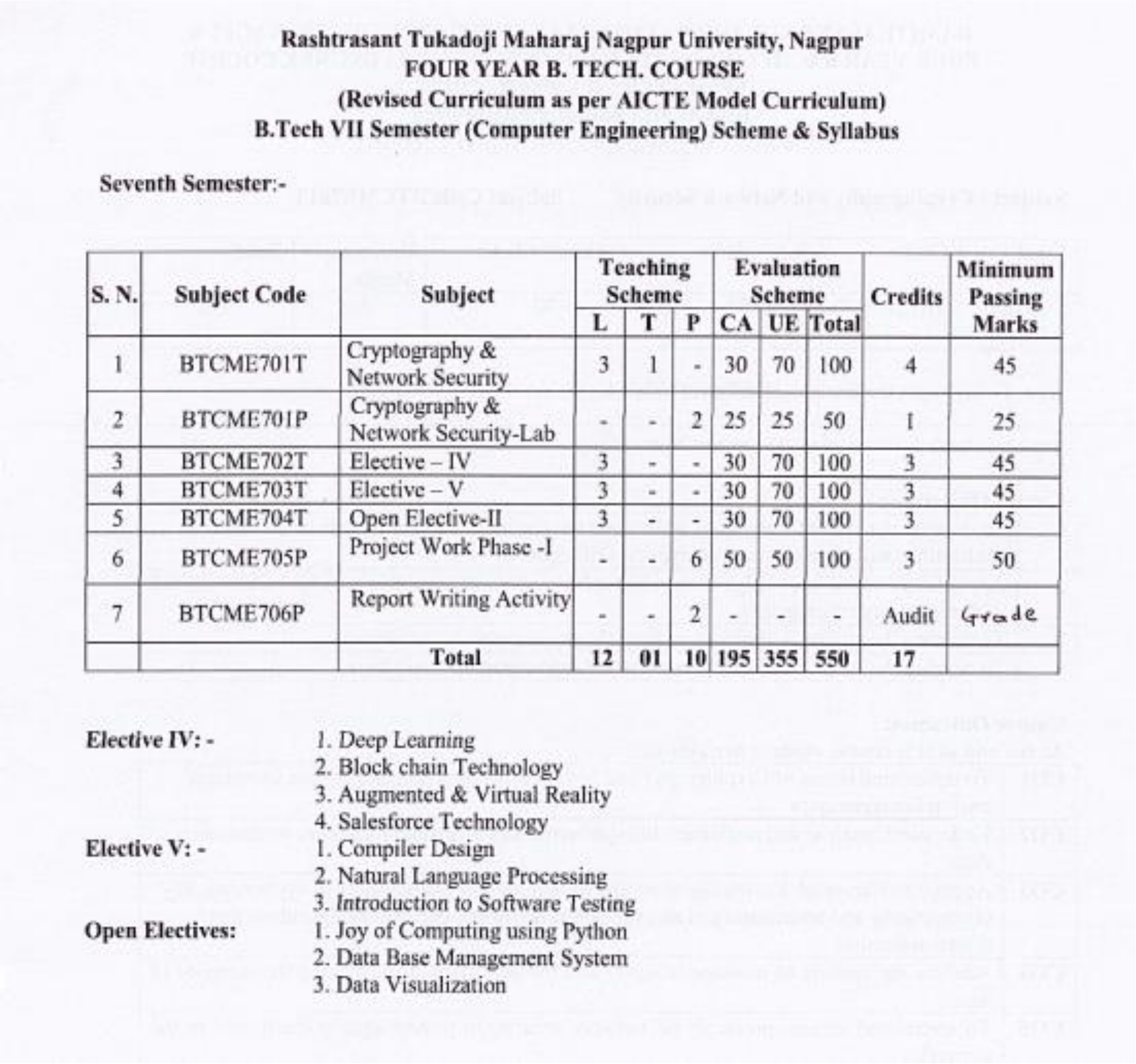
Subject Incharge: Prof. Ashvini Bais

Asst. Prof. (CE Dept.)

NOTES

CRYPTOGRAPHY & NETWORK SECURITY

Semester: 7th Sem (Final Year)



Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
FOUR YEAR B. TECH. COURSE
(Revised Curriculum as per AICTE Model Curriculum)
B.Tech VII Semester (Computer Engineering) Scheme & Syllabus

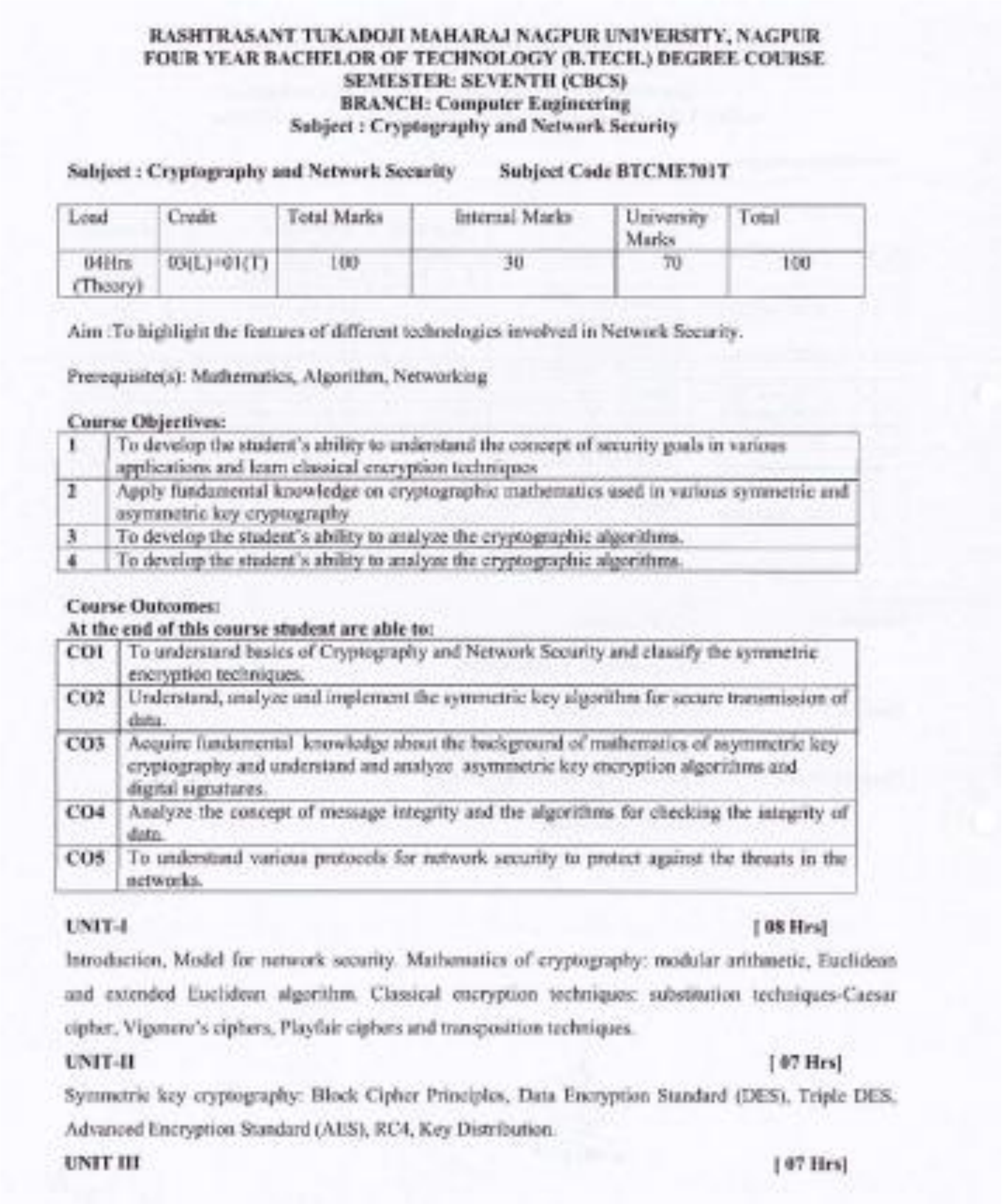
Seventh Semester:-

S. N.	Subject Code	Subject	Teaching Scheme			Evaluation Scheme			Credits	Minimum Passing Marks
			L	T	P	CA	UE	Total		
1	BTCME701T	Cryptography & Network Security	3	1	-	30	70	100	4	45
2	BTCME701P	Cryptography & Network Security-Lab	-	-	2	25	25	50	1	25
3	BTCME702T	Elective – IV	3	-	-	30	70	100	3	45
4	BTCME703T	Elective – V	3	-	-	30	70	100	3	45
5	BTCME704T	Open Elective-II	3	-	-	30	70	100	3	45
6	BTCME705P	Project Work Phase -I	-	-	6	50	50	100	3	50
7	BTCME706P	Report Writing Activity	-	-	2	-	-	-	Audit	Grade
		Total	12	01	10	195	355	550	17	

Elective IV: -
1. Deep Learning
2. Block chain Technology
3. Augmented & Virtual Reality
4. Salesforce Technology

Elective V: -
1. Compiler Design
2. Natural Language Processing
3. Introduction to Software Testing

Open Electives:
1. Joy of Computing using Python
2. Data Base Management System
3. Data Visualization



RASHTRASANT TUKADOJI MAHARAJ NAGPUR UNIVERSITY, NAGPUR
FOUR YEAR BACHELOR OF TECHNOLOGY (B.TECH.) DEGREE COURSE
SEMESTER: SEVENTH (CBCS)
BRANCH: Computer Engineering
Subject : Cryptography and Network Security

Subject : Cryptography and Network Security **Subject Code BTCME701T**

Load	Credit	Total Marks	Internal Marks	University Marks	Total
04Hrs (Theory)	03(L)+01(T)	100	30	70	100

Aim :To highlight the features of different technologies involved in Network Security.

Prerequisite(s): Mathematics, Algorithm, Networking

Course Objectives:

1	To develop the student's ability to understand the concept of security goals in various applications and learn classical encryption techniques
2	Apply fundamental knowledge on cryptographic mathematics used in various symmetric and asymmetric key cryptography
3	To develop the student's ability to analyze the cryptographic algorithms.
4	To develop the student's ability to analyze the cryptographic algorithms.

Course Outcomes:
At the end of this course student are able to:

CO1	To understand basics of Cryptography and Network Security and classify the symmetric encryption techniques.
CO2	Understand, analyze and implement the symmetric key algorithm for secure transmission of data.
CO3	Acquire fundamental knowledge about the background of mathematics of asymmetric key cryptography and understand and analyze asymmetric key encryption algorithms and digital signatures.
CO4	Analyze the concept of message integrity and the algorithms for checking the integrity of data.
CO5	To understand various protocols for network security to protect against the threats in the networks.

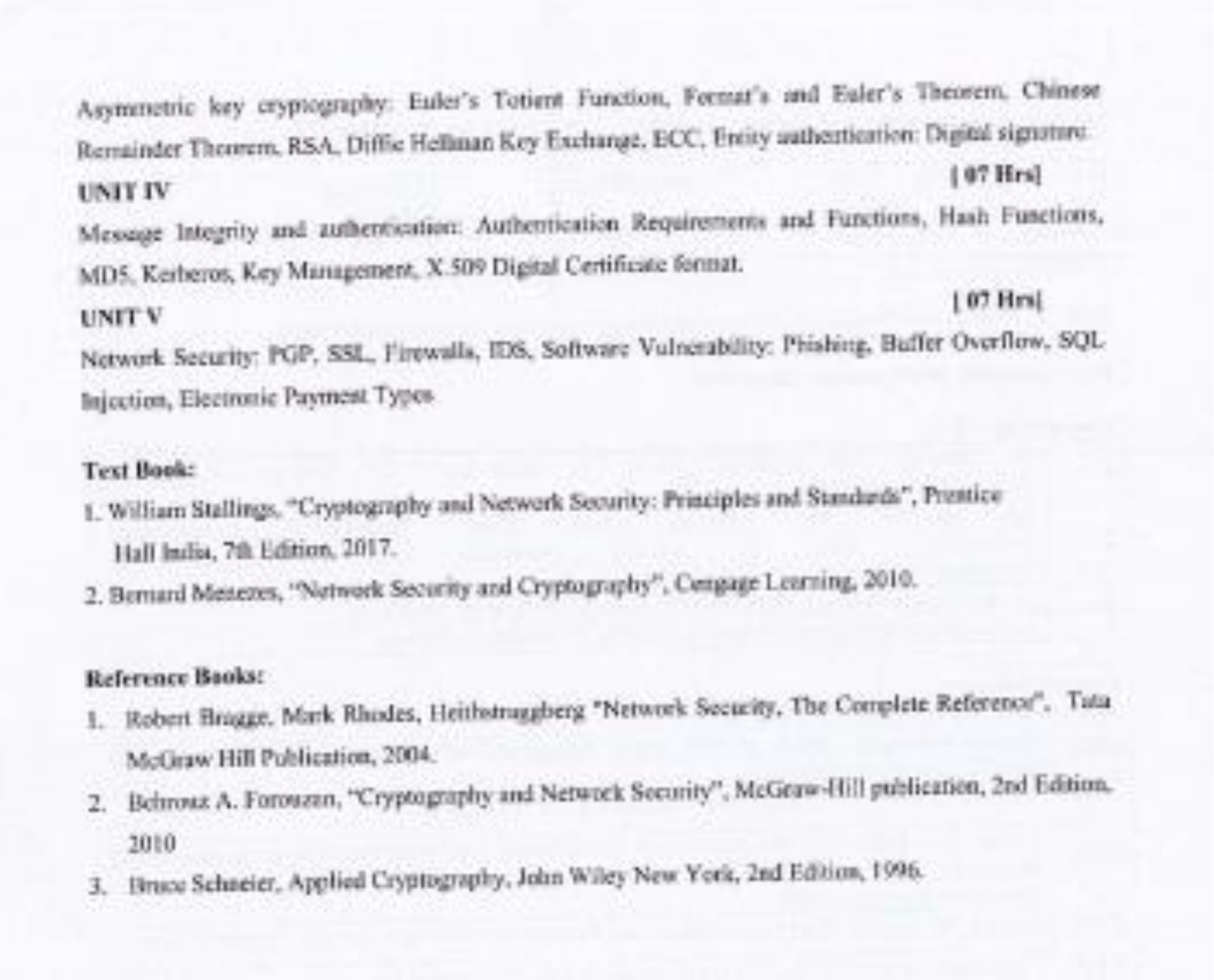
UNIT-I **[08 Hrs]**

Introduction, Model for network security. Mathematics of cryptography: modular arithmetic, Euclidean and extended Euclidean algorithm. Classical encryption techniques: substitution techniques-Caesar cipher, Vigenere's ciphers, Playfair ciphers and transposition techniques.

UNIT-II **[07 Hrs]**

Symmetric key cryptography: Block Cipher Principles, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), RC4, Key Distribution.

UNIT III **[07 Hrs]**



Asymmetric key cryptography: Euler's Totient Function, Fermat's and Euler's Theorem, Chinese Remainder Theorem, RSA, Diffie Hellman Key Exchange, ECC, Entity authentication: Digital signature

UNIT IV **[07 Hrs]**

Message Integrity and authentication: Authentication Requirements and Functions, Hash Functions, MD5, Kerberos, Key Management, X.509 Digital Certificate format.

UNIT V **[07 Hrs]**

Network Security: PGP, SSL, Firewalls, IDS, Software Vulnerability: Phishing, Buffer Overflow, SQL Injection, Electronic Payment Types

Text Book:

1. William Stallings, "Cryptography and Network Security: Principles and Standards", Prentice Hall India, 7th Edition, 2017.
2. Bernard Menezes, "Network Security and Cryptography", Cengage Learning, 2010.

Reference Books:

1. Robert Bragge, Mark Rhodes, Heithstraggberg "Network Security, The Complete Reference", Tata McGraw Hill Publication, 2004.
2. Behrouz A. Forouzan, "Cryptography and Network Security", McGraw-Hill publication, 2nd Edition, 2010
3. Bruce Schneier, Applied Cryptography, John Wiley New York, 2nd Edition, 1996.

UNIT V

Network Security: PGP, SSL, Firewalls, IDS, Software Vulnerability: Phishing, Buffer Overflow, SQL Injection, Electronic Payment Types.

Network Security

PGP-

Pretty Good Privacy (PGP) is an encryption system used for both sending encrypted emails and encrypting sensitive files. Since its invention back in 1991, PGP has become the de facto standard for email security.

The popularity of PGP is based on two factors. The first is that the system was originally available as freeware, and so spread rapidly among users who wanted an extra level of security for their email messages. The second is that since PGP uses both symmetric encryption and public-key encryption, it allows users who have never met to send encrypted messages to each other without exchanging private encryption keys.

PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann. PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email. PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.

PGP is an open source and freely available software package for email security. PGP provides authentication through the use of Digital Signature. It provides confidentiality through the use of symmetric block encryption. It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

PGP (Pretty Good Privacy)**,** is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage. It was designed by Phil Zimmermann way back in 1991. He designed it in such a way, that the best cryptographic algorithms such as RSA, Diffie-Hellman key exchange, DSS are used for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA are used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open source one and is not dependent on either the OS (Operating System) or the processor. The application is based on a few commands which are very easy to use.

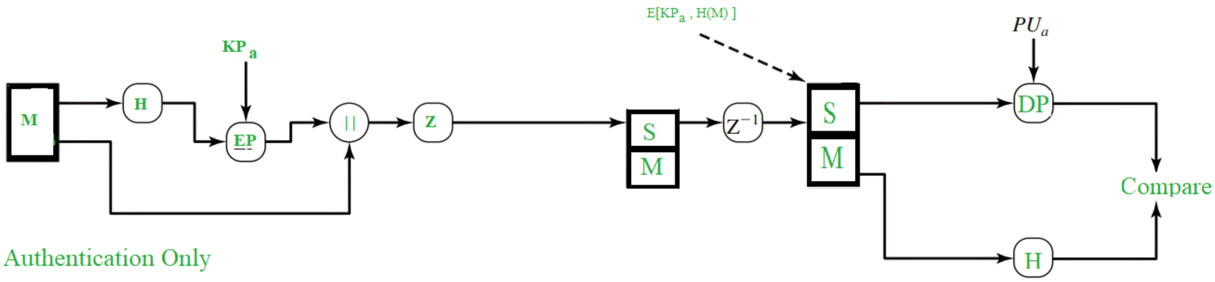
The following are the services offered by PGP:

1. Authentication
2. Confidentiality
3. Compression
4. Email Compatibility
5. Segmentation

Authentication:

Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure.

In the email world, checking the authenticity of an email is nothing but to check whether it actually came from the person it says. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience. The Authentication service in PGP is provided as follows:



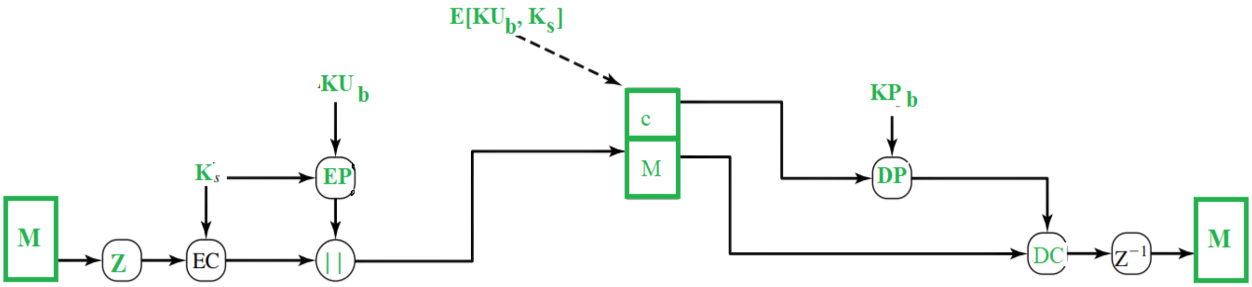
As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message. For the hashing purpose, SHA-1 is used and it produces a 160 bit output hash value. Then, using the sender's private key (KP_a), it is encrypted and it's called as Digital Signature. The Message is then appended to the signature. All the process happened till now, is sometimes described as signing the message. Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.

At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key(PU_a) and the hash value is obtained. The message is again passed to hash function and it's hash value is calculated and obtained. Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it's not a legit one.

Confidentiality:

Sometimes we see some packages labelled as 'Confidential', which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

PGP provides that Confidentiality service in the following manner:



Only Confidentiality

The message is first compressed and a 128 bit session key (K_s), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (K_s) itself gets encrypted through public key encryption (EP) using receiver's public key(KU_b) . Both the encrypted entities are now concatenated and sent to the receiver.

As you can see, the original message was compressed and then encrypted initially and hence even if any one could get hold of the traffic, he cannot read the contents as they are not in readable form and they can only read them if they had the session key (K_s). Even though session key is transmitted to the receiver and hence, is in the traffic, it is in encrypted form and only the receiver's private key (KP_b)can be used to decrypt that and thus our message would be completely safe.

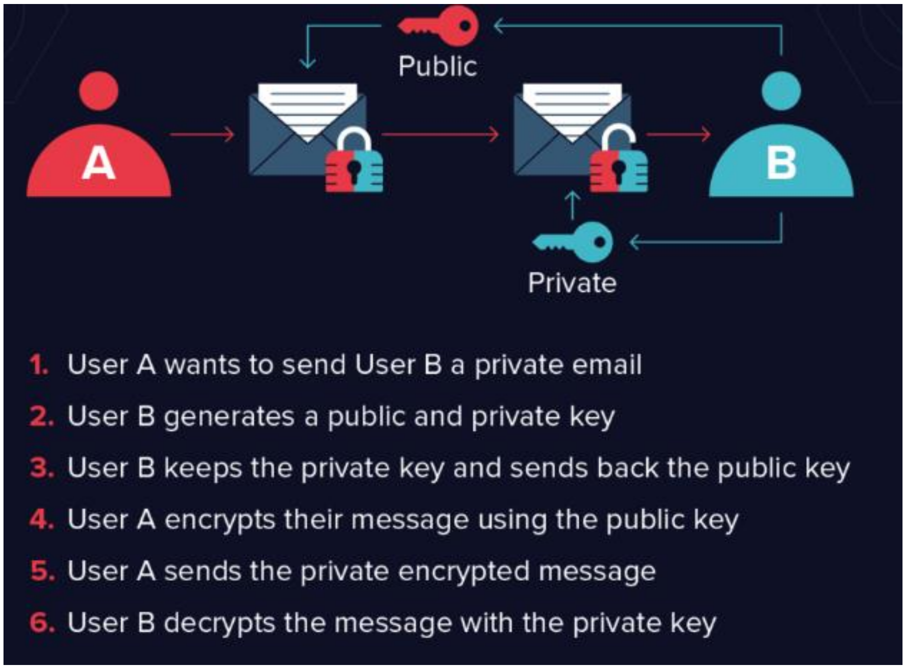
At the receiver's end, the encrypted session key is decrypted using receiver's private key (KP_b) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M).
RSA algorithm is used for the public-key encryption and for the symmetric key encryption, CAST-128(or IDEA or 3DES) is used.

How Does PGP Encryption Work?

First, PGP generates a random session key using one of two (main) algorithms. This key is a huge number that cannot be guessed, and is only used once.

Next, this session key is encrypted. This is done using the public key of the intended recipient of the message. The public key is tied to a particular person's identity, and anyone can use it to send them a message.

The sender sends their encrypted PGP session key to the recipient, and they are able to decrypt it using their private key. Using this session key, the recipient is now able to decrypt the actual message.



1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

Disadvantages of PGP Encryption:

1. **The Administration is difficult**: The different versions of PGP complicate the administration.

2. **Compatibility issues**: Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.

3. **Complexity**: PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.

4. **No Recovery**: Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

Secure Socket Layer (SSL)-

In year 1995, Netscape developed SSLv2 and used in Netscape Navigator 1.1. The SSL version1 was never published and used. Later, Microsoft improved upon SSLv2 and introduced another similar protocol named Private Communications Technology (PCT).

Netscape substantially improved SSLv2 on various security issues and deployed SSLv3 in 1999. The Internet Engineering Task Force (IETF) subsequently, introduced a similar TLS (Transport Layer Security) protocol as an open standard. TLS protocol is non-interoperable with SSLv3.

TLS modified the cryptographic algorithms for key expansion and authentication. Also, TLS suggested use of open crypto Diffie-Hellman (DH) and Digital Signature Standard (DSS) in place of patented RSA crypto used in SSL. But due to expiry of RSA patent in 2000, there existed no strong reasons for users to shift away from the widely deployed SSLv3 to TLS.

Salient Features of SSL:

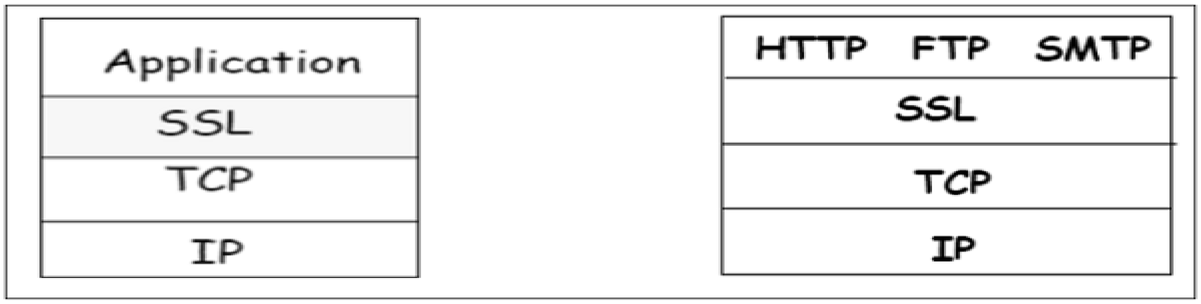
The salient features of SSL protocol are as follows −

- SSL provides network connection security through −
  - **Confidentiality** − Information is exchanged in an encrypted form.
  - **Authentication** − Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
  - **Reliability** − Maintains message integrity checks.
- SSL is available for all TCP applications.
- Supported by almost all web browsers.
- Provides ease in doing business with new online entities.
- Developed primarily for Web e-commerce.

Architecture of SSL:

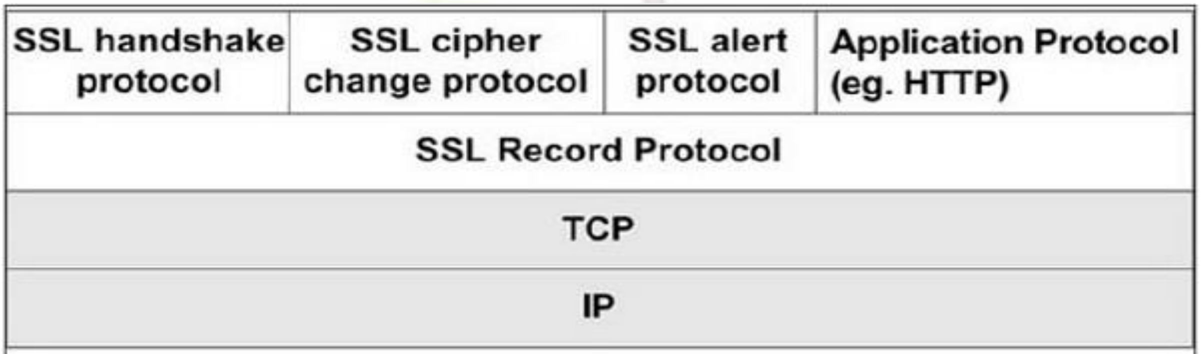
SSL is specific to TCP and it does not work with UDP. SSL provides Application Programming Interface (API) to applications. C and Java SSL libraries/classes are readily available.

SSL protocol is designed to interwork between application and transport layer as shown in the following image −



SSL itself is not a single layer protocol as depicted in the image; in fact it is composed of two sub-layers.

- Lower sub-layer comprises of the one component of SSL protocol called as SSL Record Protocol. This component provides integrity and confidentiality services.
- Upper sub-layer comprises of three SSL-related protocol components and an application protocol. Application component provides the information transfer service between client/server interactions. Technically, it can operate on top of SSL layer as well. Three SSL related protocol components are −
  - SSL Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert Protocol.
- These three protocols manage all of SSL message exchanges and are discussed later in this section.

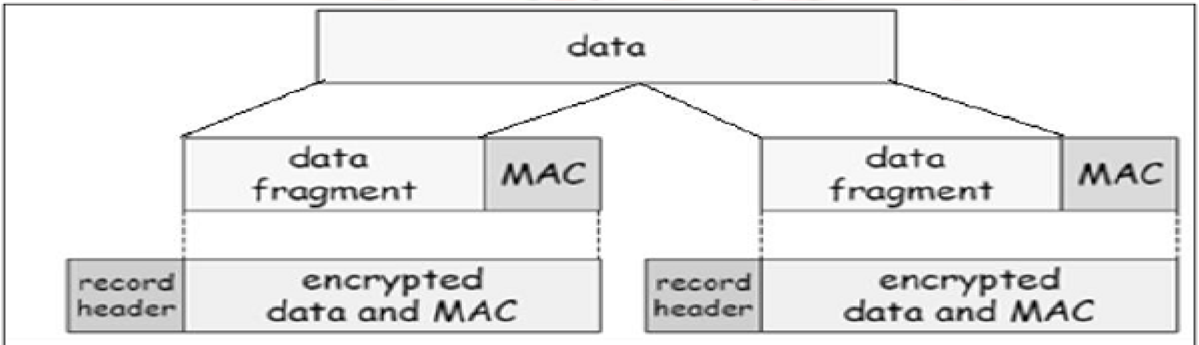


SSL Protocol Architecture

Functions of SSL Protocol Components:

The four sub-components of the SSL protocol handle various tasks for secure communication between the client machine and the server.

- **Record Protocol**
  - The record layer formats the upper layer protocol messages.
  - It fragments the data into manageable blocks (max length 16 KB). It optionally compresses the data.
  - Encrypts the data.
  - Provides a header for each message and a hash (Message Authentication Code (MAC)) at the end.
  - Hands over the formatted blocks to TCP layer for transmission.



Data formatting by SSL Record protocol

- **SSL Handshake Protocol**
  - It is the most complex part of SSL. It is invoked before any application data is transmitted. It creates SSL sessions between the client and the server.
  - Establishment of session involves Server authentication, Key and algorithm negotiation, Establishing keys and Client authentication (optional).
  - A session is identified by unique set of cryptographic security parameters.
  - Multiple secure TCP connections between a client and a server can share the same session.
  - Handshake protocol actions through four phases. These are discussed in the next section.
- **Change Cipher Spec Protocol**
  - Simplest part of SSL protocol. It comprises of a single message exchanged between two communicating entities, the client and the server.

  - As each entity sends the Change Cipher Spec message, it changes its side of the connection into the secure state as agreed upon.
  - The cipher parameters pending state is copied into the current state.
  - Exchange of this Message indicates all future data exchanges are encrypted and integrity is protected.

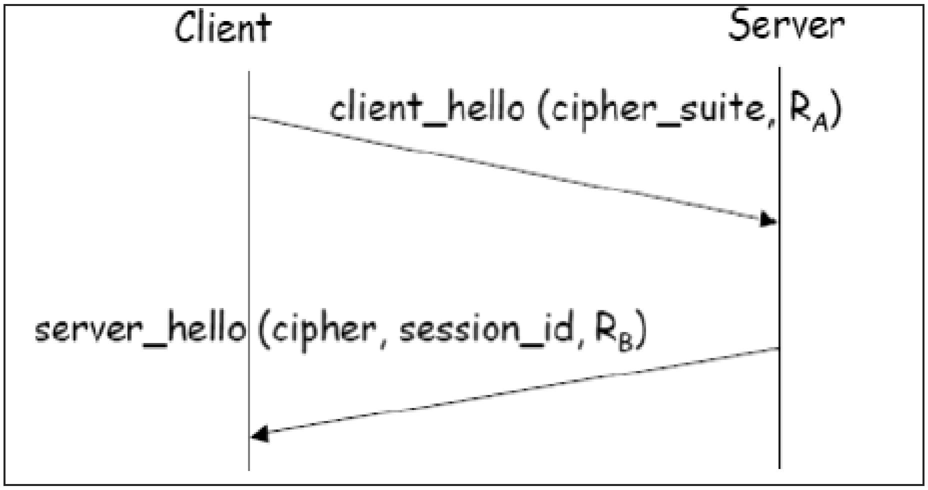
- **SSL Alert Protocol**
  - This protocol is used to report errors – such as unexpected message, bad record MAC, security parameters negotiation failed, etc.
  - It is also used for other purposes – such as notify closure of the TCP connection, notify receipt of bad or unknown certificate, etc.

Establishment of SSL Session:

As discussed above, there are four phases of SSL session establishment. These are mainly handled by SSL Handshake protocol.

Phase 1 − Establishing security capabilities.

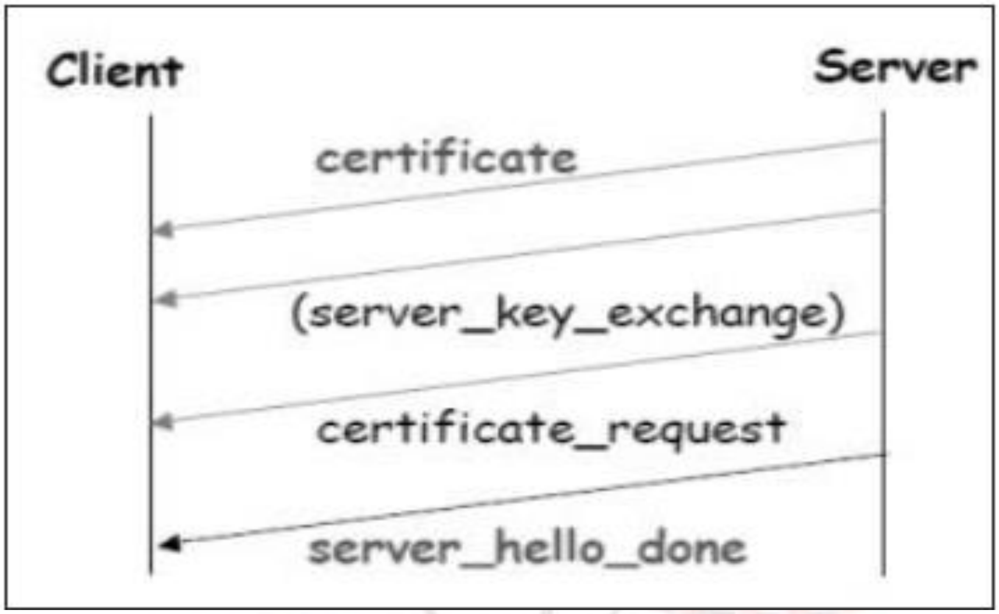
- This phase comprises of exchange of two messages – *Client_hello* and *Server_hello*.


Client
Server
client_hello (cipher_suite, R_A)
server_hello (cipher, session_id, R_B)

- *Client_hello* contains of list of cryptographic algorithms supported by the client, in decreasing order of preference.
- *Server_hello* contains the selected Cipher Specification (CipherSpec) and a new *session_id*.
- The CipherSpec contains fields like −
  - Cipher Algorithm (DES, 3DES, RC2, and RC4)

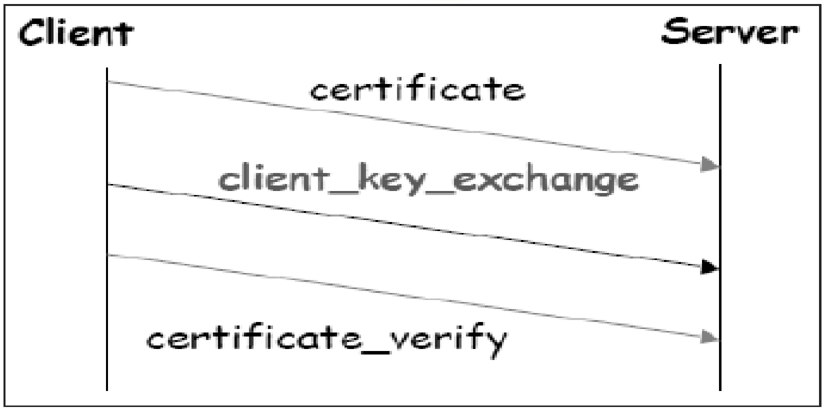
- MAC Algorithm (based on MD5, SHA-1)
- Public-key algorithm (RSA)
- Both messages have “nonce” to prevent replay attack.

Phase 2 − Server authentication and key exchange.



- Server sends certificate. Client software comes configured with public keys of various “trusted” organizations (CAs) to check certificate.
- Server sends chosen cipher suite.
- Server may request client certificate. Usually it is not done.
- Server indicates end of *Server_hello*.

Phase 3 − Client authentication and key exchange.

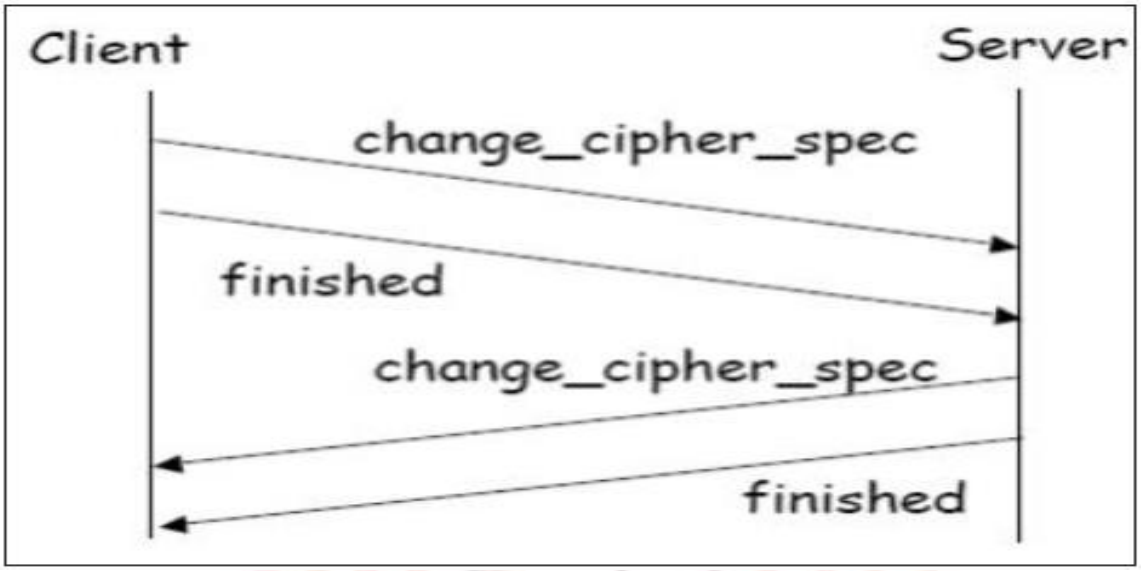


- Client sends certificate, only if requested by the server.

- It also sends the Pre-master Secret (PMS) encrypted with the server's public key.

- Client also sends *Certificate_verify* message if certificate is sent by him to prove he has the private key associated with this certificate. Basically, the client signs a hash of the previous messages.

Phase 4 − Finish.



- Client and server send *Change_cipher_spec* messages to each other to cause the pending cipher state to be copied into the current state.

- From now on, all data is encrypted and integrity protected.

- Message "Finished" from each end verifies that the key exchange and authentication processes were successful.

All four phases, discussed above, happen within the establishment of TCP session. SSL session establishment starts after TCP SYN/ SYNACK and finishes before TCP Fin.

Resuming a Disconnected Session

- It is possible to resume a disconnected session (through *Alert*message), if the client sends a *hello_request* to the server with the encrypted *session_id* information.

- The server then determines if the *session_id* is valid. If validated, it exchanges ChangeCipherSpec and *finished* messages with the client and secure communications resume.

- This avoids recalculating of session cipher parameters and saves computing at the server and the client end.

SSL Session Keys:

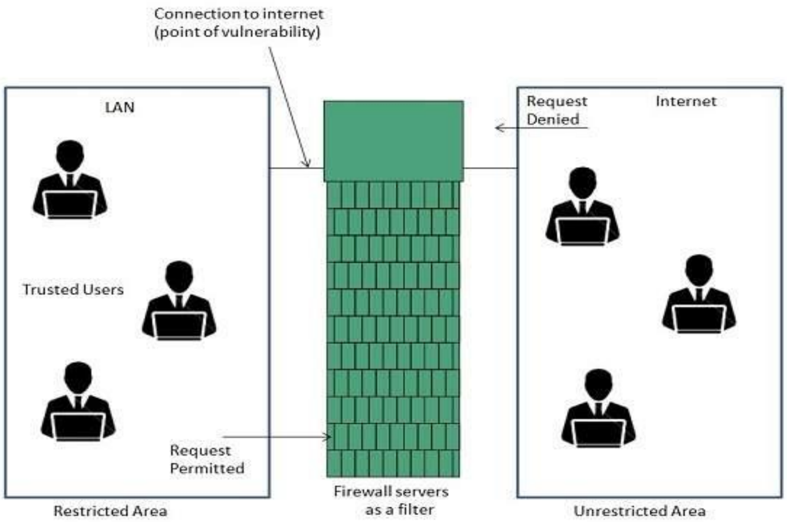
We have seen that during Phase 3 of SSL session establishment, a pre-master secret is sent by the client to the server encrypted using server's public key. The master secret and various session keys are generated as follows −

- The master secret is generated (via pseudo random number generator) using −
  - The pre-master secret.
  - Two nonces (RA and RB) exchanged in the client_hello and server_hello messages.
- Six secret values are then derived from this master secret as −
  - Secret key used with MAC (for data sent by server)
  - Secret key used with MAC (for data sent by client)
  - Secret key and IV used for encryption (by server)
  - Secret key and IV used for encryption (by client)

Firewalls-

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



There are two types of Firewall system: One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

Key Points

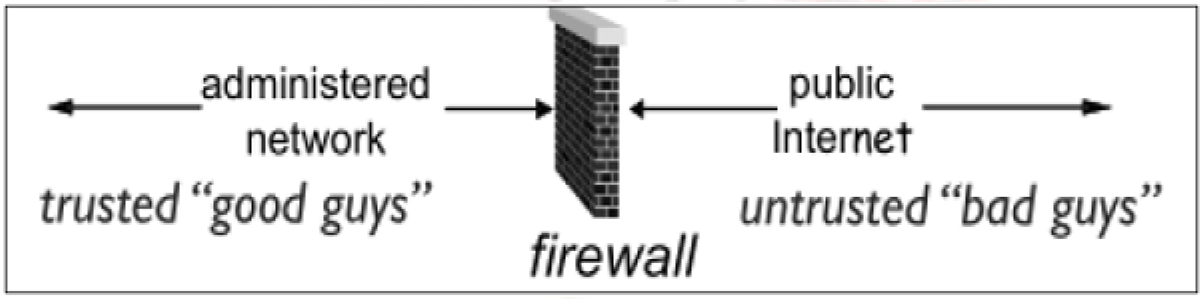
- Firewall management must be addressed by both system managers and the network managers.
- The amount of filtering a firewall varies. For the same firewall, the amount of filtering may be different in different directions.

Almost every medium and large-scale organization has a presence on the Internet and has an organizational network connected to it. Network partitioning at the boundary between the outside Internet and the internal network is essential for network security. Sometimes the inside network (intranet) is referred to as the “trusted” side and the external Internet as the “un-trusted” side.

Types of Firewall:

Firewall is a network device that isolates organization’s internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.

All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.



Deploying firewall at network boundary is like aggregating the security at a single point. It is analogous to locking an apartment at the entrance and not necessarily at each door.

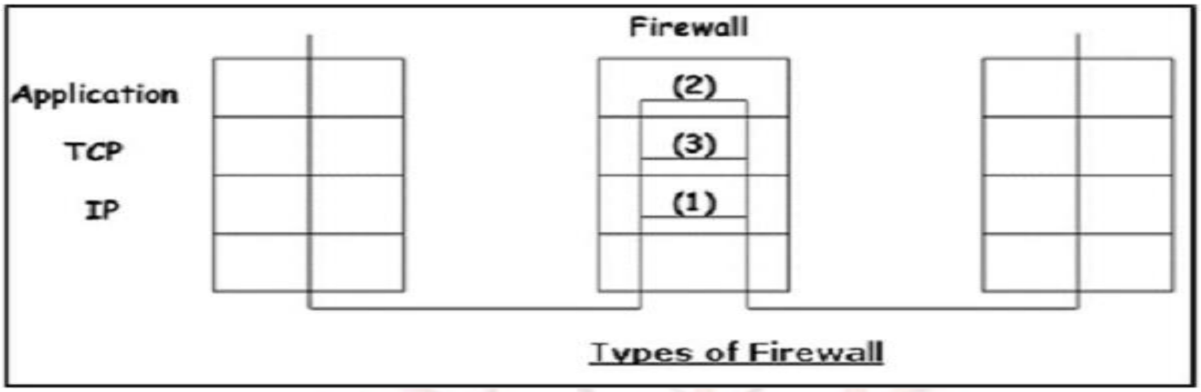
Firewall is considered as an essential element to achieve network security for the following reasons −

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

Firewall is categorized into three basic types −

- Packet filter (Stateless & Stateful)
- Application-level gateway
- Circuit-level gateway

These three categories, however, are not mutually exclusive. Modern firewalls have a mix of abilities that may place them in more than one of the three categories.



Packet Filtering Firewalls:

Packet Filtering Firewalls are normally deployed on the Routers which connect the Internal Network to Internet. Packet Filtering Firewalls can only be implemented on the Network Layer of IOS Model. Packet Filtering Firewalls work on the Basis of Rules defines by Access Control Lists. They check all the Packets and screen them against the rules defined by the Network Administrator as per the ACLs. If in case, any packet does not meet the criteria then that packet is dropped and Logs are updated about this information.

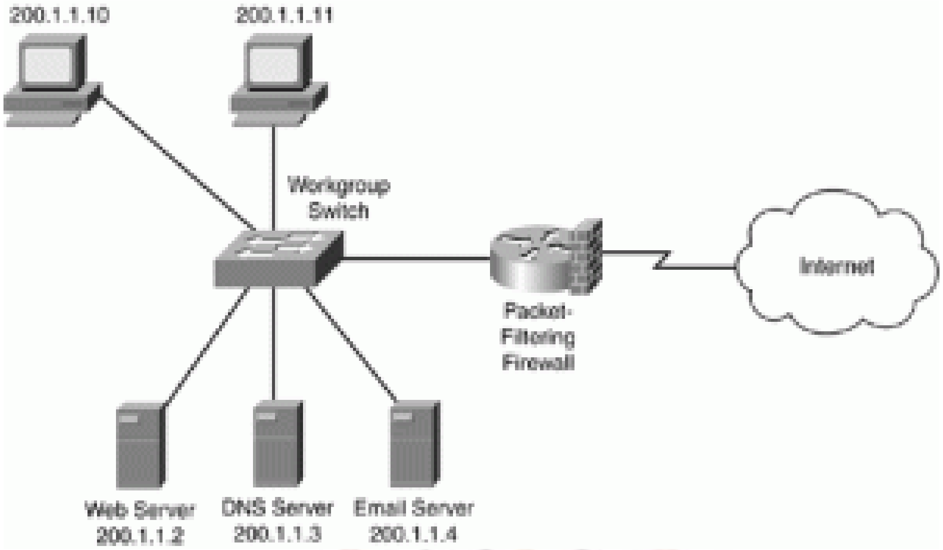
Administrators can create their ACLs on the basis Address, Protocols and Packet attributes.

Advantage:

The Biggest Advantage of Packet Filtering Firewalls is Cost and Lower Resource Usage and best suited for Smaller Networks.

Disadvantage:

Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule-based models. And it’s also Vulnerable to Spoofing in some Cases.



Circuit level gateways firewalls:

Circuit level gateways firewalls are deployed at the Session layer of the OSI model and they monitor sessions like TCP three-way handshake to see whether a requested connection is legitimate or not. Major Screening happens before the Connection is established. Information sent to a Computer outside the network through a circuit level gateway appears to have originated from the Gateway. This helps in creating a stealth cover for the private network from outsiders.

Advantage:

Circuit level gateways are comparatively inexpensive and provide Anonymity to the private network.

Disadvantage:

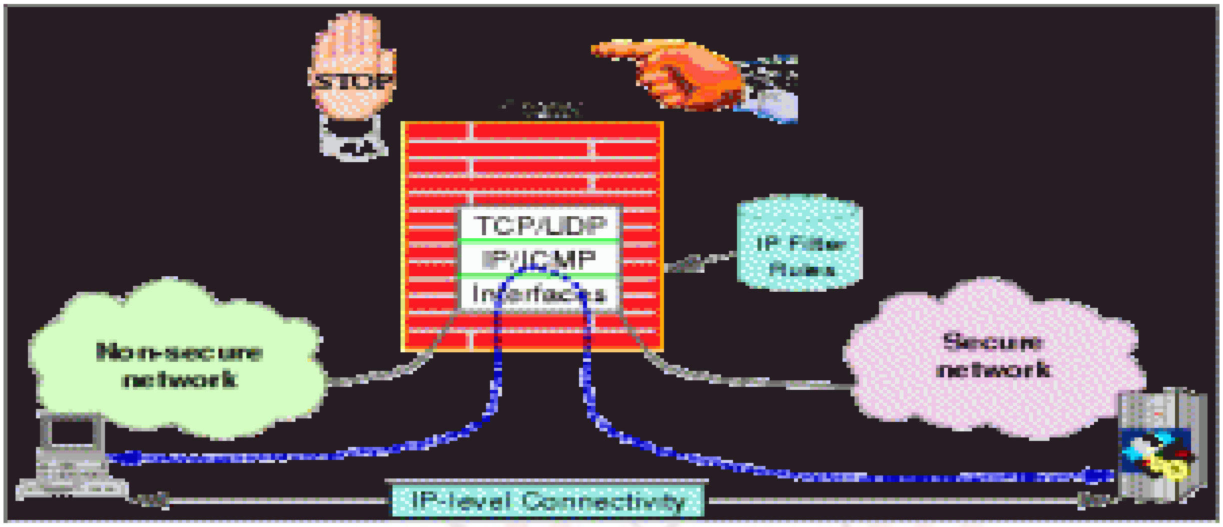
Circuit level Gateways do not filter Individual Packets. After Establishing a Connection, an Attacker may take advantage of this.

Application level gateways firewalls:

Application level gateways firewalls work on the Application layer of the OSI model and provide protection for a specific Application Layer Protocols. Proxy server is the best example of Application Level Gateways Firewalls. Application level gateway would work only for the protocols which are configured. For example, if we install a web proxy-based Firewall than it will only allow HTTP Protocol Data. They are supposed to understand application specific commands such as HTTP: GET and HTTP: POST as they are deployed on the Application Layer, for a Specific Protocol. Application level firewalls can also be configured as Caching Servers which in turn increase the network performance and makes it easier to log traffic.

Advantages:

Application inspection firewalls can prevent more kinds of attacks than stateful firewalls can. For example, application inspection firewalls can stop an attacker from trying to set up a virtual private network (VPN) tunnel (triggered from inside the network) through an application firewall by way of tunneled HTTP requests.



Stateful multilayer Inspection Firewall:

Stateful multilayer Inspection Firewall is a combination of all the firewalls that we have studied till now. They can filter packets at Network layer using ACLs, check for legitimate sessions on the Session Layers and they also evaluate packets on the Application layer (ALG).

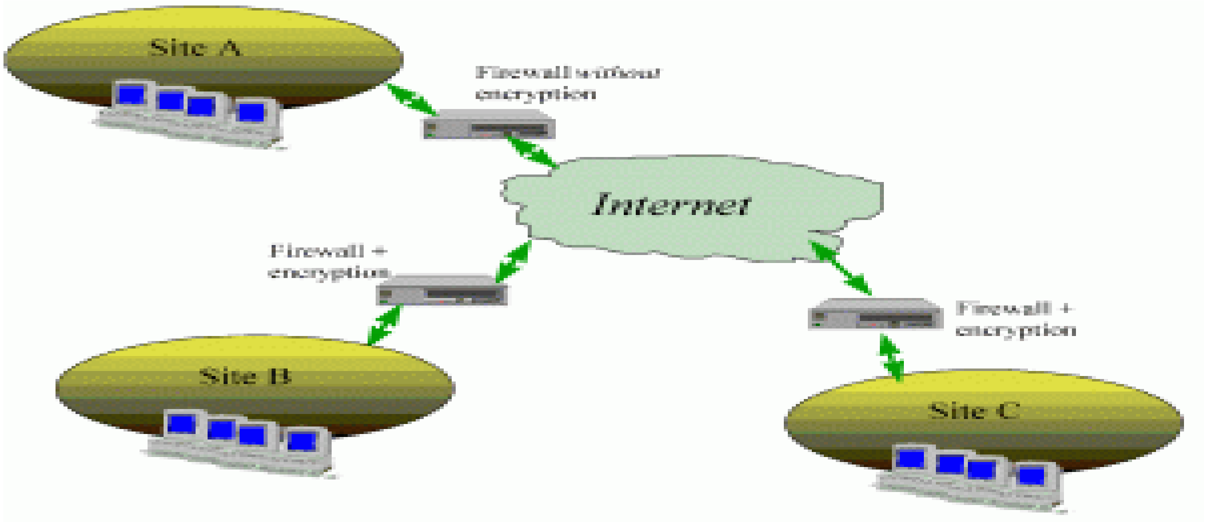
Advantages:

Stateful Multilayer Inspection Firewall can work on a transparent mode allowing direct connections between the client and the server which was earlier not possible. It can also implement algorithms and complex security models which are protocol specific, making the connections and data transfer more secure.

Overview of firewalls:

Generally, firewalls examine all the data packets passing through them to see if they meet the rules defined by the ACL (Access Control List) made by the administrator of the network. Only if the Data Packets are allowed as per ACL, they will be transmitted over the Connection.

Firewalls generally also maintain a log of Important Activities inside the Network. A Network Administrator can define what is important for him and configure the Firewall to make the Logs accordingly. Firewall can filter contents on the basis of Address, Protocols, Packet attributes, State, and it’s generally only Screen the Packet Headers.



Firewall Characteristics:

- All traffic from inside to outside and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. The configurations used for this are screened Host Firewall (Single and Dual) and Screened Subnet Firewall.
- Only authorized traffic as defined by the local security policy will be allowed to pass. Various types of firewalls that can be used are Packet-Filters, Stateful Filters and Application Proxy Filters.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Techniques for Control:

Four general techniques that firewalls use to control access and enforce security policy are as follows

- Service Control- This determines the types of internet services that can be accessed inbound or outbound.
- Direction Control: This determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- User Control: Control access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter.

- Behaviour Control: Controls how particular services are used.

Capabilities of Firewalls:

The expectations from a firewall are as follows

- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits vulnerability and provides protection from spoofing and routing attacks.
- A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several internet functions that are not security related which include network address translator and a network management function.
- A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Limitations of Firewalls:

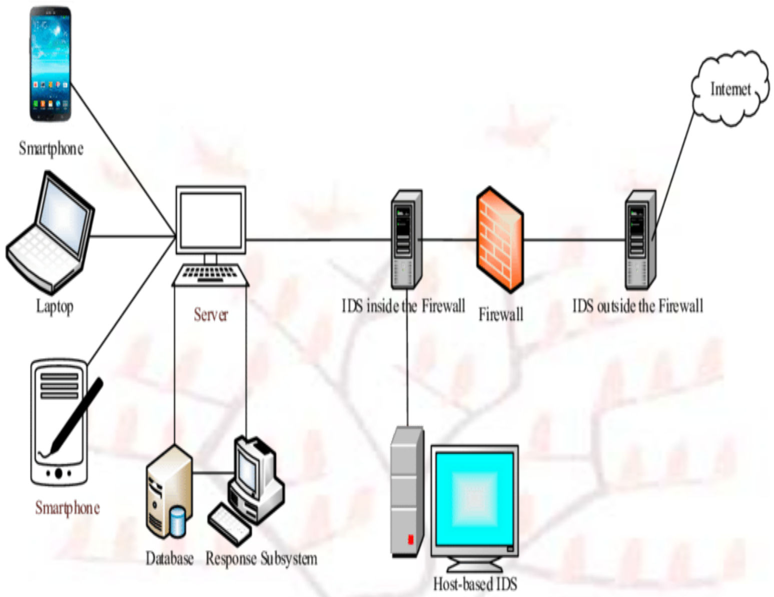
- The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modern pool that provides dial-in capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter it would be impractical and impossible for the firewall to scan all incoming files for viruses.

Design Goals:

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration. This implies the use of a trusted system with a secure operating system.

Intrusion Detection System (IDS)-

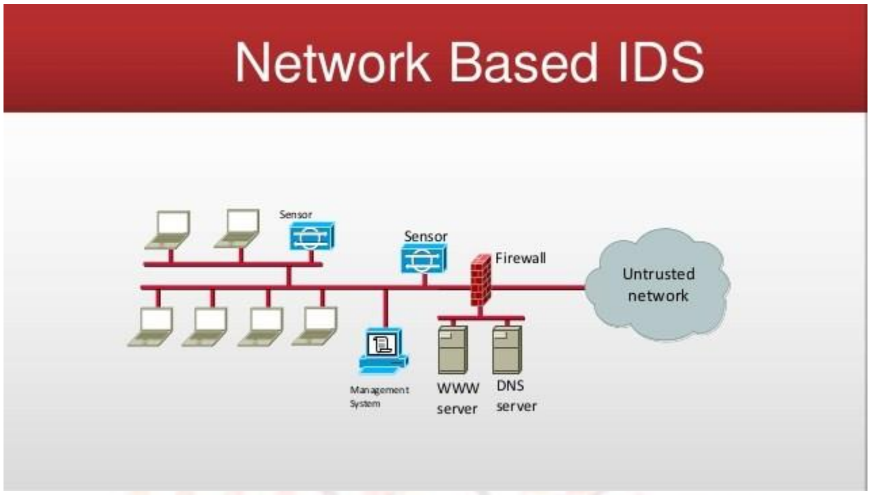
An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.



While there are several types of IDS, ranging in scope from single computers to large networks, the most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

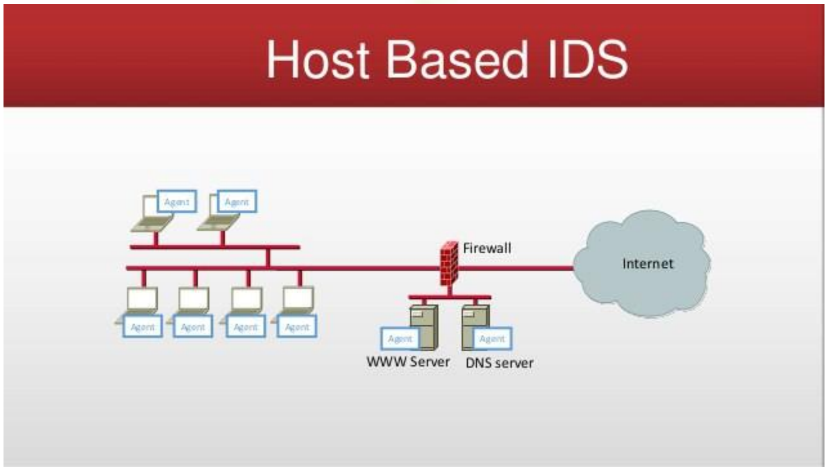
Network intrusion detection systems:

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulating network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.


Network Based IDS

Host intrusion detection systems:

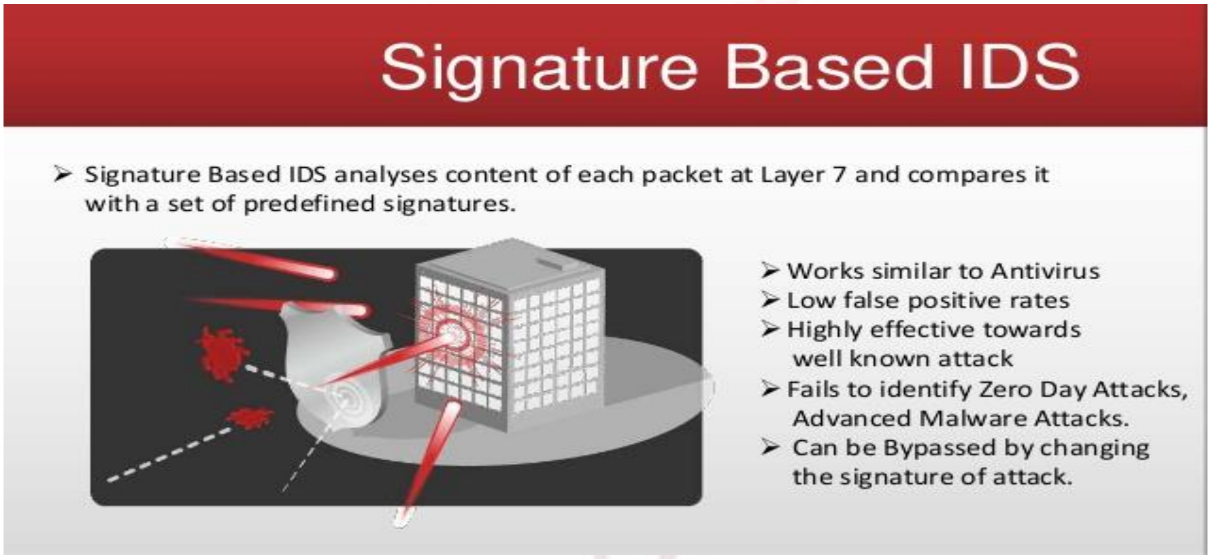
Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.


Host Based IDS

Detection method-

Signature-based:

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available. Signature based IDS is very helpful for detecting already known attacks.



Signature Based IDS

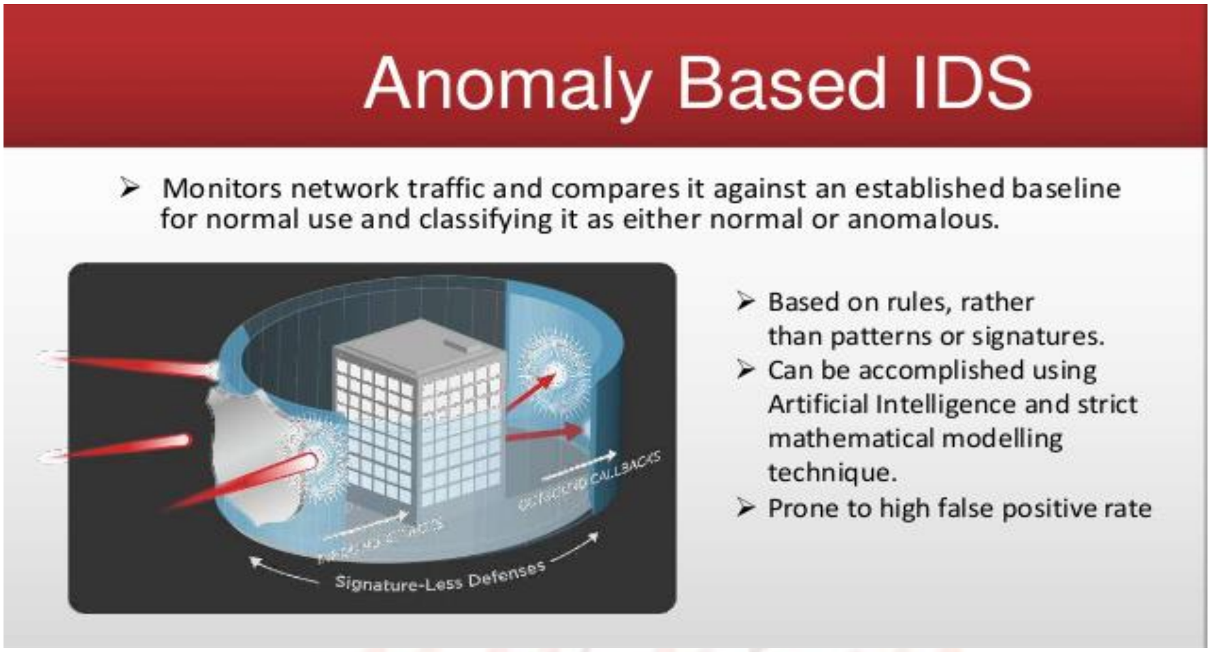
- Signature Based IDS analyses content of each packet at Layer 7 and compares it with a set of predefined signatures.

- Works similar to Antivirus
- Low false positive rates
- Highly effective towards well known attack
- Fails to identify Zero Day Attacks, Advanced Malware Attacks.
- Can be Bypassed by changing the signature of attack.

Anomaly-based:

Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious.

New types of what could be called anomaly-based intrusion detection systems are being viewed by Gartner as User and Entity Behavior Analytics (UEBA) (an evolution of the user behavior analytics category) and network traffic analysis (NTA). In particular, NTA deals with malicious insiders as well as targeted external attacks that have compromised a user machine or account. Gartner has noted that some organizations have opted for NTA over more traditional IDS.



Anomaly Based IDS

- Monitors network traffic and compares it against an established baseline for normal use and classifying it as either normal or anomalous.

- Based on rules, rather than patterns or signatures.
- Can be accomplished using Artificial Intelligence and strict mathematical modelling technique.
- Prone to high false positive rate

OUTBOUND CALLBACKS
INBOUND ATTACKS
Signature-Less Defenses

Different types of intrusion detection systems:

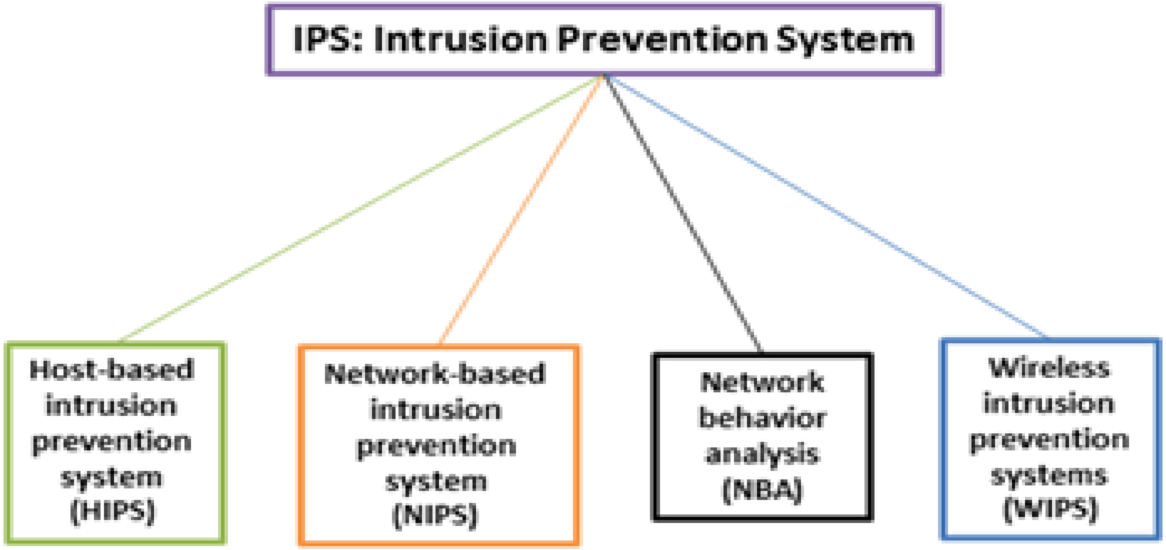
Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- A network intrusion detection system (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

- Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.

- Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.

- Anomaly-based intrusion detection systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.


IPS: Intrusion Prevention System
Host-based intrusion prevention system (HIPS)
Network-based intrusion prevention system (NIPS)
Network behavior analysis (NBA)
Wireless intrusion prevention systems (WIPS)

Historically, intrusion detection systems were categorized as passive or active; a passive IDS that detected malicious activity would generate alert or log entries, but would take no actions. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems, and a version is available for Windows as well.

Capabilities of intrusion detection systems:

Intrusion detection systems monitor network traffic in order to detect when an intrusion is being carried out by unauthorized entities. IDSes do this by providing some or all of these functions to security professionals:

- monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks;
- providing administrators a way to tune, organize and understand relevant operating system audit trails and other logs that are often otherwise difficult to track or parse;
- providing a user-friendly interface so non-expert staff members can assist with managing system security;
- including an extensive attack signature database against which information from the system can be matched;

- recognizing and reporting when the IDS detects that data files have been altered;
- generating an alarm and notifying that security has been breached; and
- reacting to intruders by blocking them or blocking the server.

An intrusion detection system may be implemented as a software application running on customer hardware, or as a network security appliance; cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

Benefits of intrusion detection systems:

Intrusion detection systems offer organizations a number of benefits, starting with the ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks, and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks.

Intrusion detection systems can also help the enterprise attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements.

Intrusion detection systems can also improve security response. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the operating systems of services being used. Using an IDS to collect this information can be much more efficient that manual censuses of connected systems.

Software Vulnerability

Phishing-

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

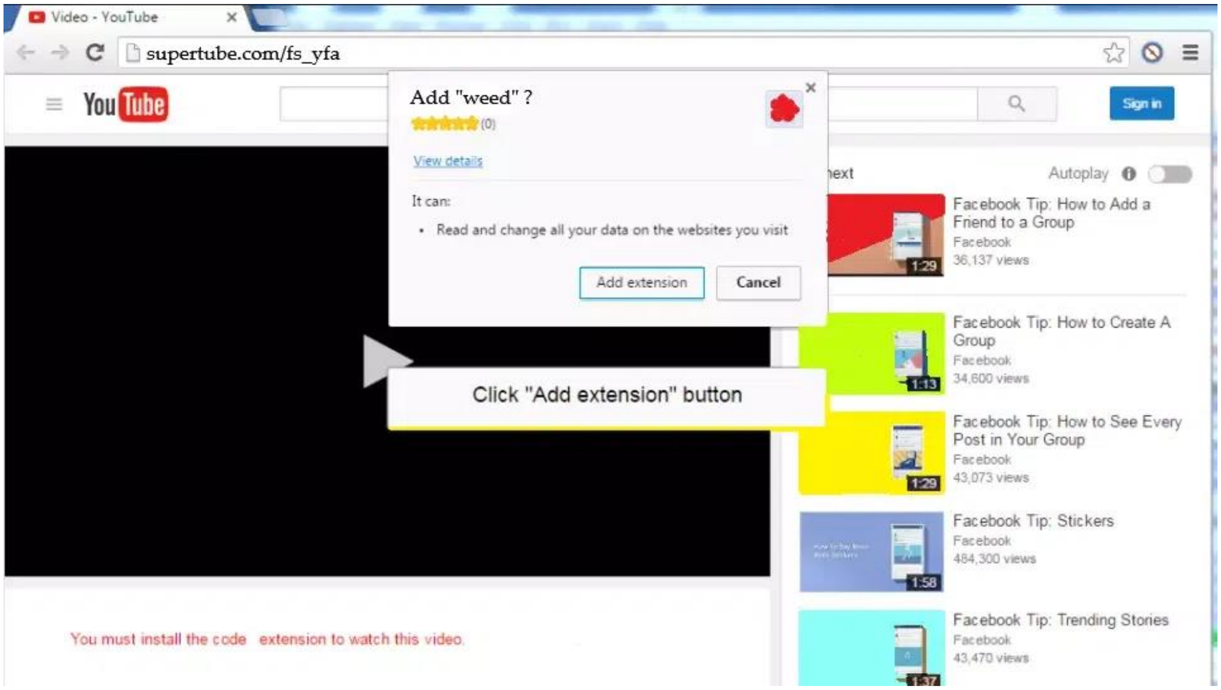
Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

Phishing emails can hit an organisation of any size and type. You might get caught up in a mass campaign (where the attacker is just looking to collect some new passwords or make some easy money), or it could be the first step in a targeted attack against your company, where the aim could be something much more specific, like the theft of sensitive data. In a targeted campaign, the attacker may use information about your employees or company to make their messages even more persuasive and realistic. This is usually referred to as spear phishing.

Phishing is one type of cyber-attack. Phishing got its name from "**phish**" meaning fish. It's a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim. The main motive of the attacker behind phishing is to gain confidential information like

- Password
- Credit card details
- Social security numbers
- Date of birth

The attacker uses this information to further target the user and impersonate the user and cause data theft. The most common type of phishing attack happens through email. Phishing victims are tricked into revealing information that they think should be kept private. The original logo of the email is used to make the user believe that it is indeed the original email. But if we carefully look into the details, we will find that the URL or web address is not authentic. Let's understand this concept with the help of an example:



Add "weed" ?

It can:

- Read and change all your data on the websites you visit

Click "Add extension" button

You must install the code extension to watch this video.

In this example, most people believe it's YouTube just by looking at the red icon. So, thinking of YouTube as a secure platform, the users click on the extension without being suspicious about it. But if we look carefully, we can see the URL is supertube.com and not youtube.com. Secondly, YouTube never asks to add extensions for watching any video. The third thing is the extension name itself is weird enough to raise doubt about its credibility.

How Does Phishing Occur?

Below mentioned are the ways through which Phishing generally occurs. Upon using any of the techniques mentioned below, the user can lead to Phishing Attacks.

- Clicking on an unknown file or attachment**:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
- Using an open or free wifi hotspot**:** This is a very simple way to get confidential information from the user by luring him by giving him free wifi**.** The wifi owner can control the user's data without the user knowing it.
- Responding to social media requests: This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistake made by naive users.
- Clicking on unauthenticated links or ads: Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

Types of Phishing Attacks

There are several types of Phishing Attacks, some of them are mentioned below. Below mentioned attacks are very common and mostly used by the attackers.

- **Email Phishing:** The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.

- **Spear Phishing:** In spear phishing of phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let's assume an employee from the finance department of some organization). Then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.

- **Whaling:** Whaling is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. a pressurized email is sent to such executives so that they don't have much time to think, therefore falling prey to phishing.

- **Smishing:** In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user id/ password, etc. Then using this information the attacker harms the victim.

- **Vishing:** Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or confidential data from the victim.

- **Clone Phishing:** Clone Phishing this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

Impact of Phishing

These are the impacts on the user upon affecting the Phishing Attacks. Each person has their own impact after getting into Phishing Attacks, but these are some of the common impacts that happen to the majority of people.

- **Financial Loss:** Phishing attacks often target financial information, such as credit card numbers and bank account login credentials. This information can be used to steal money or make unauthorized purchases, leading to significant financial losses.

- **Identity Theft:** Phishing attacks can also steal personal information, such as Social Security numbers and date of birth, which can be used to steal an individual's identity and cause long-term harm.

- **Damage to Reputation:** Organizations that fall victim to phishing attacks can suffer damage to their reputation, as customers and clients may lose trust in the company's ability to protect their information.

- **Disruption to Business Operations:** Phishing attacks can also cause significant disruption to business operations, as employees may have their email accounts or computers compromised, leading to lost productivity and data.

- **Spread of Malware:** Phishing attacks often use attachments or links to deliver malware, which can infect a victim’s computer or network and cause further harm.

Signs of Phishing

It is very much important to be able to identify the signs of a phishing attack in order to protect against its harmful effects. These signs help the user to protect user data and information from hackers. Here are some signs to look out for include:

- **Suspicious email addresses:** Phishing emails often use fake email addresses that appear to be from a trusted source, but are actually controlled by the attacker. Check the email address carefully and look for slight variations or misspellings that may indicate a fake address.

- **Urgent requests for personal information:** Phishing attacks often try to create a sense of urgency in order to trick victims into providing personal information quickly. Be cautious of emails or messages that ask for personal information and make sure to verify the authenticity of the request before providing any information.

- **Poor grammar and spelling:** Phishing attacks are often created quickly and carelessly, and may contain poor grammar and spelling errors. These mistakes can indicate that the email or message is not legitimate.

- **Requests for sensitive information:** Phishing attacks often try to steal sensitive information, such as login credentials and financial information. Be cautious of emails or messages that ask for sensitive information and verify the authenticity of the re
quest before providing any information.

- **Unusual links or attachments:** Phishing attacks often use links or attachments to deliver malware or redirect victims to fake websites. Be cautious of links or attachments in emails or messages, especially from unknown or untrusted sources.

- **Strange URLs:** Phishing attacks often use fake websites that look similar to the real ones, but have slightly different URLs. Look for strange URLs or slight variations in the URL that may indicate a fake website.

How To Stay Protected Against Phishing?

Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:

- **Authorized Source:** Download software from authorized sources only where you have trust.

- **Confidentiality:** Never share your private details with unknown links and keep your data safe from hackers.

- **Check URL:** Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.

- **Avoid replying to suspicious things:** If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.

- **Phishing Detection Tool:** Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.

- **Try to avoid free wifi:** Avoid using free Wifi, it will lead to threats and Phishing.

- **Keep your system updated:** It's better to keep your system always updated to protect from different types of Phishing Attacks.

- **Keep the firewall of the system ON:** Keeping ON the firewalls helps you in filtering ambiguous and suspicious data and only authenticated data will reach to you.

Buffer OverFlow-

A buffer is a temporary area for data storage. When more data (than was originally allocated to be stored) gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.

In a buffer-overflow attack**,** the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information. Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input. There are two types of buffer overflows: stack-based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack memory space used to store user input.

A buffer overflow attack is a common cyberattack that deliberately exploits a buffer overflow vulnerability where user-controlled data is written to memory. By submitting more data than can fit in the allocated memory block, the attacker can overwrite data in other parts of memory.

Types of Buffer Overflow Attacks-

A buffer overflow attack can be performed in a few different ways, but some of the most common examples include:

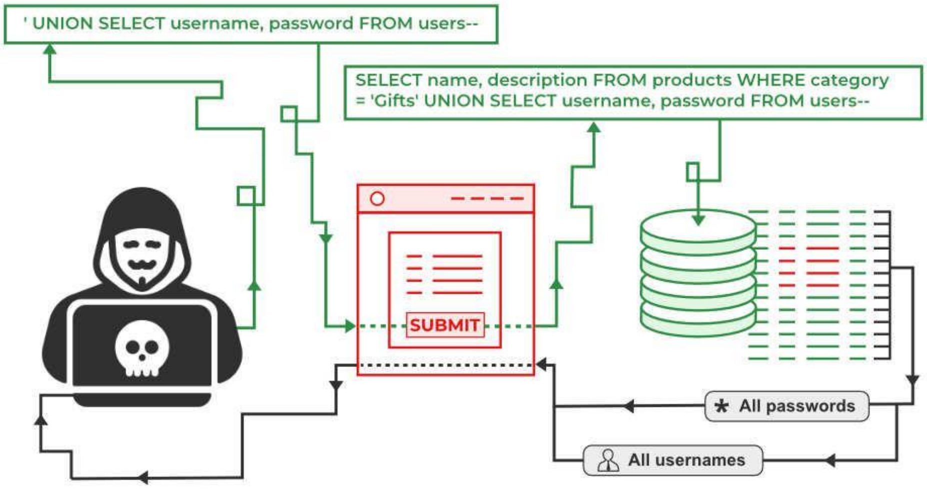
- **Stack-Based Buffer Overflow:** The program stack contains critical control flow data for an application — such as function return pointers — and is a common target of buffer overflow attacks. Overwriting a return pointer can cause the program to jump to attacker-controlled data and execute it as code, allowing the attacker to run code with the same permissions as the application.
- **Heap-Based Buffer Overflow:** The program heap is used to dynamically allocate memory to variables whose size is not defined when the program compiles. By exploiting a buffer overflow vulnerability and flooding the system heap, an attacker can overwrite critical application data.
- **Format String Attacks:** Functions in the printf family in C/C++ can use format strings, which allow reading and writing of memory. If user-provided data is interpreted as a format string, it can be used to leak or modify sensitive values.

SQL Injection-

SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. According to the Open Web Application Security Project, injection attacks, which include SQL injections, were the third most serious web application security risk in 2021.

SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server.

1. SQL injection is a code injection technique that can compromise your database.
2. SQL injection is one of the most common web hacking techniques.
3. SQL injection is the injection of malicious code into SQL statements via web page input.


' UNION SELECT username, password FROM users--
SELECT name, description FROM products WHERE category = 'Gifts' UNION SELECT username, password FROM users--
SUBMIT
All passwords
All usernames

Electronic Payment Types-

Electronic payments are payments that are made directly to the payee from your bank accounts using security features over the Internet to process the transactions. Electronic payments start with an arrangement you make with your financial institutions to have funds withdrawn from your account and sent to a payee.

An electronic payment is any kind of non-cash payment that doesn't involve a paper check. Methods of electronic payments include credit cards, debit cards and the ACH (Automated Clearing House) network. The ACH system comprises direct deposit, direct debit and electronic checks (e-checks). For all these methods of electronic payment, there are three main types of transactions:

1. A one-time customer-to-vendor payment is commonly used when you shop online at an e-commmerce site, such as Amazon. You click on the shopping cart icon, type in your credit card information and click on the checkout button. The site processes your credit card information and sends you an e-mail notifiying you that your payment was received. On some Web sites, you can use an e-check instead of a credit card. To pay by e-check, you type in your account number and your bank's routing number. The vendor authorizes payment through the customer's bank, which then either initiates an electronic funds transfer (EFT) or prints a check and mails it to the vendor.

2. You make a recurring customer-to-vendor payment when you pay a bill through a regularly scheduled direct debit from your checking account or an automatic charge to your credit card. This type of payment plan is commonly offered by car insurance companies, phone companies and loan management companies. Some long-term contracts (like those at gyms or fitness centers) require this type of automated payment schedule.

3. To use automatic bank-to-vendor payment, your bank must offer a service called online bill pay. You log on to your bank's Web site, enter the vendor's information and authorize your bank to electronically transfer money from your account to pay your bill. In most cases, you can choose whether to do this manually for each billing cycle or have your bills automatically paid on the same day each month.