NETWORKING SECURITY

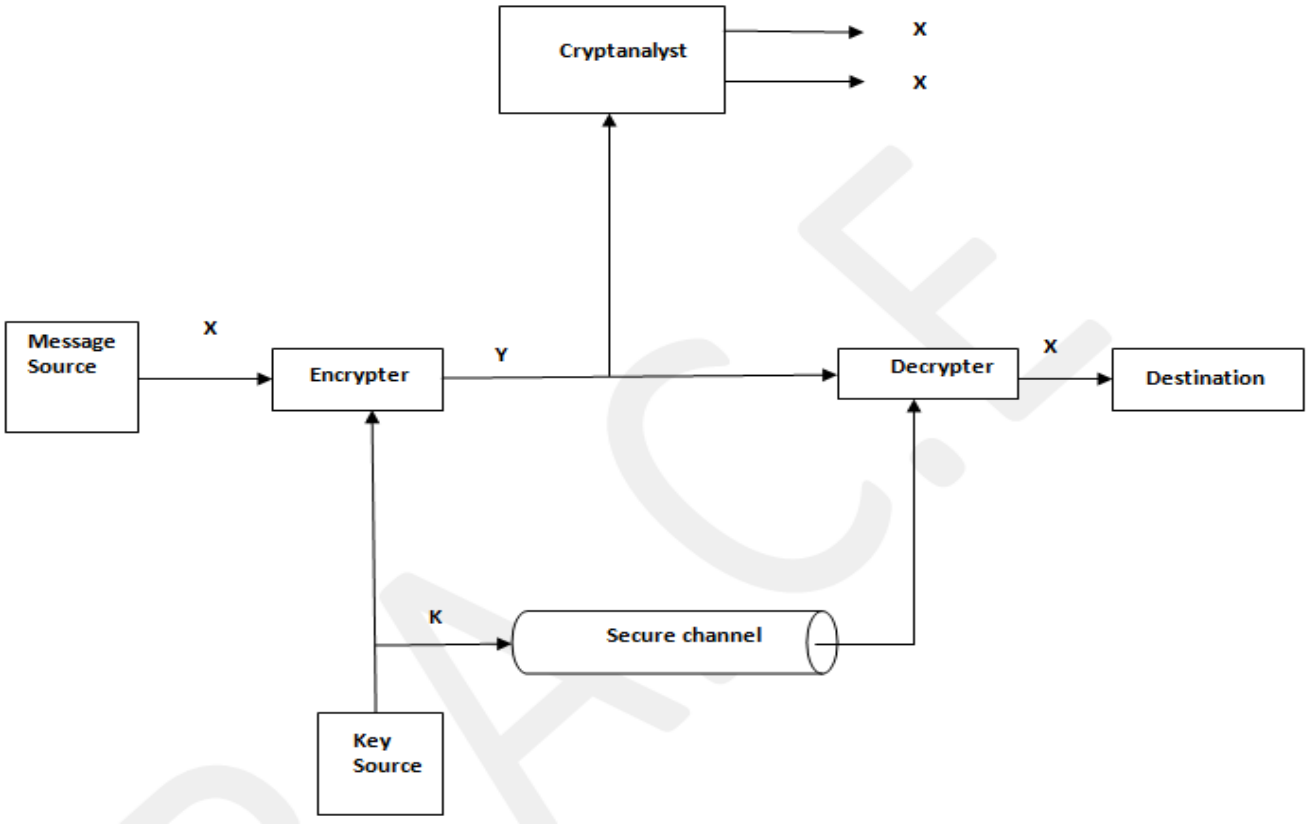
CONVENTIONAL ENCRYPTION

The conventional encryption process. The original intelligence message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext that controls the algorithm. The algorithm will producers different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm. The security of conventional encryption depends on several factors. First, the encryption algorithm must be powerful enough so that it is impractical to decrypt a message on the basis of the cipher text alone. Beyond that, the security of conventional encryption depends on the secrecy of the key, not on the secrecy of the algorithm. That is, it is assumed that it is impractical to decrypt a message on the basis of the cipher text plus knowledge of the encryption / decryption algorithm. In other words, we don't need to keep the algorithm secret. We only need to keep the key secret. The fact that the algorithm need not be kept secret means that manufacture can and have developed low – cost chip implementations of data encryption algorithms. These chips are when available and incorporated into a number of products. With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key.

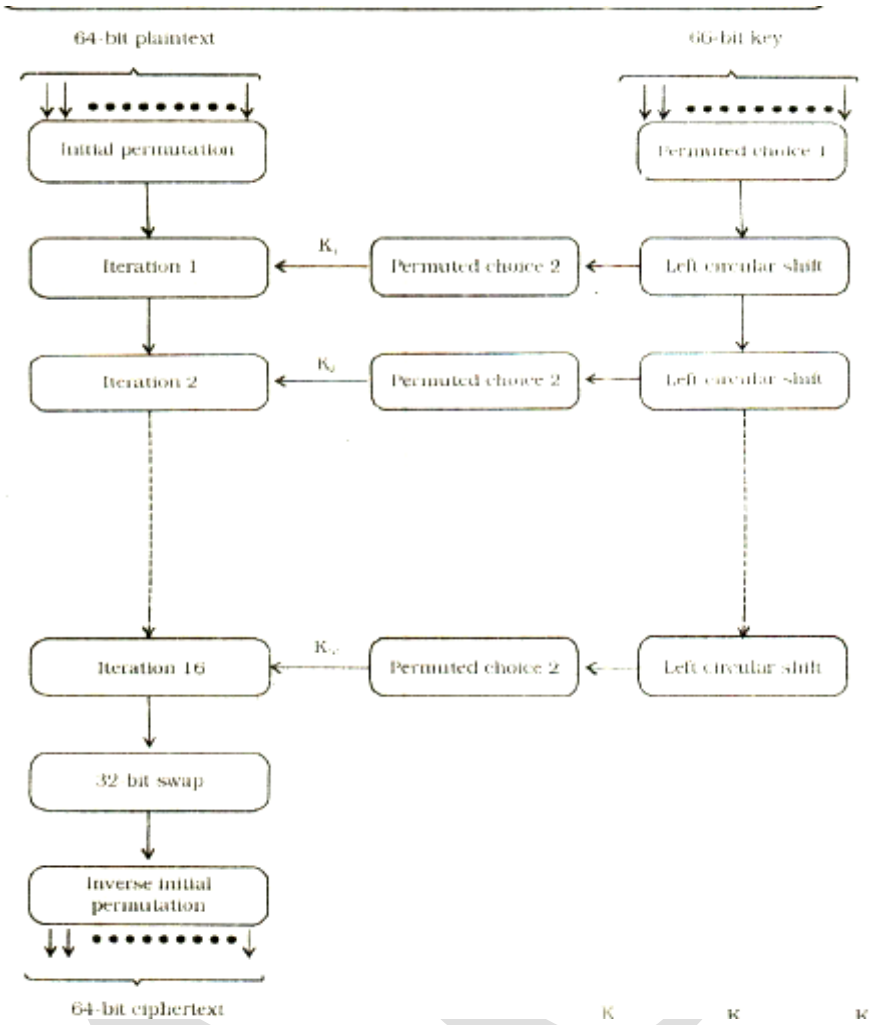
DATA ENCRYPTION STANDARD (DES)

The overall scheme for DES encryption is illustrated in Figure. As with any encryption scheme; there are two inputs to the encryption function; the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length, and the key is 56 bits in length.

The processing of the plaintext proceeds in three phases. First, the 64 – bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This IP is followed by phase consisting of 16 iterations of the same function. The output of the last (16^{th}) iteration consists of 64 bits that are a function of the plaintext input and the key. The left and right halves of the output are swapped to produce the pre - output. Finally, the preoutput is passed through a permutation (IP – I) that is the inverse of the initial permutation function, in order to produce the 64 – bit cipher text.



Model of Conventional Cryptosystem

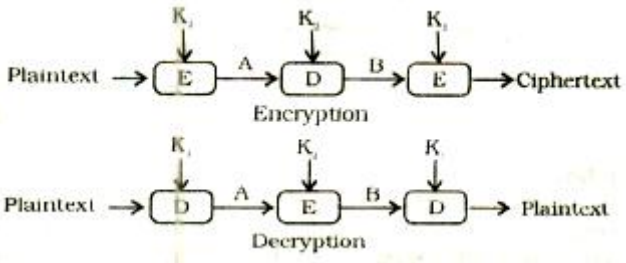


Triple DES

Triple DES was first proposed by Tuchman [TUCH79], and first standardized for use in financial applications [ANSI85]. Triple DES uses two keys and three executions of the DES algorithm. The function below an encrypt – decrypt – encrypt (EDE) sequence:

$$C = E_{K1}[D_{K1}[E_{K1}[P]]] = E_{K1}[P]$$

Although only two keys are used, three instances of the DES algorithm are required. It turns out than there is a simple technique, known as a meet – in – the middle attack that would reduce a double DES system with two keys to the relative strength of ordinary single DES.



With three iterations of the DES function, the effective key length is 112bits.

The strength of DES

The focus of concern has been on the eight substitution tables, or S – boxes, that are used in each iteration because the design criteria for these boxes, and indeed for the entire algorithm, have never been made public, there is a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an opponent who knows the weakness in the S – boxes. The assertion is tantalizing, and over the years a number of regularities unexpected behaviors of the S –boxes have been discovered.

Despite this problem, no one has so far succeeded in discovering the supposed fatal weaknesses in the S – boxes. Indeed, as advances in cryptanalytic techniques have occurred, the underlying strength of the DES algorithm has become more apartment. As of this writing, no practical attack method for DES has been published. Given that the algorithm has survived years of intensive scrutiny unscathed, it is probably safe to say that DES is one of the strongest encryption algorithms ever devised.

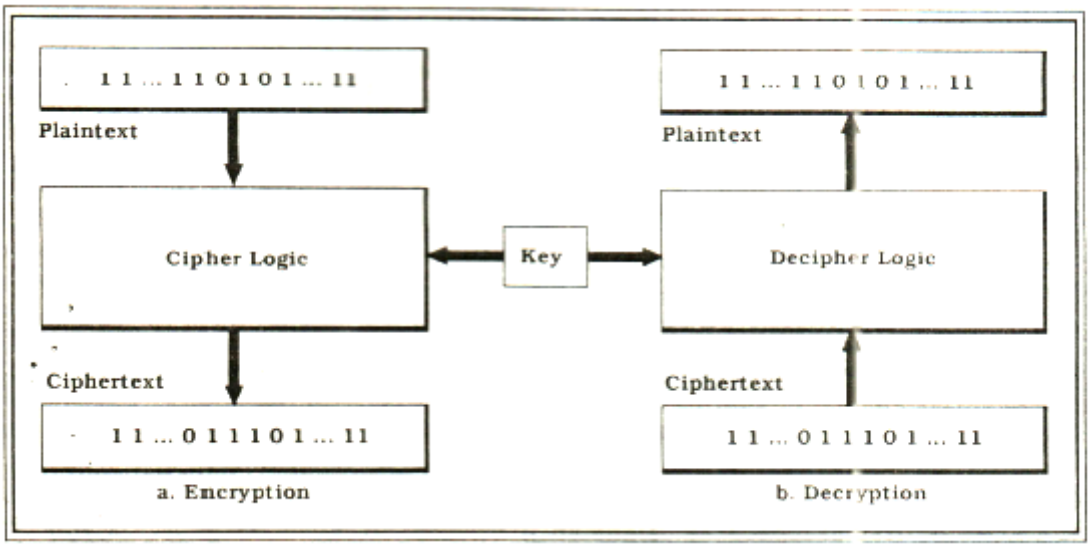
CRYPTANALYSIS

The cryptanalysis deals with listening to the cipher text while cryptography is concerned with designing a cipher (key) to allow intruder to inject or modify the cipher text. Sometimes these two processes are collectively known as cryptology. The encryption key is a short string of characters, and one potential encryption key is selected out of the string. For analog or text communication, the key may be string of characters, but in digital communication, the key is a binary string. Depending on the application, the key may be kept secret in additional security or the key and encryption algorithm together may be kept secret (for additional security)

Block Cipher

Traditional ciphers used a character or symbol as the unit of encryption / decryption. Modem ciphers on the other hand, use a block of bits as the unit of encryption / decryption. The concept of the block cipher, the plaintext and cipher text are block of bits.

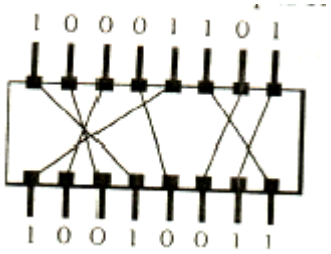
A P – box (P for permutation) performs a transposition at the bit level; it transposes bits. It can be implemented in software or hardware, but hardware



Block Cipher

P - box

DES takes the data and chops them into 8 – byte segments. However, the encryption and the key are the same for each segment. So if the data are four equal segments, the result is also four equal segments.



Diagram

PRIVATE – KEY AND PUBLIC – KEY CRYPTOGRAPHY

Private – key cryptography required distribution of secret keys over an insecure communication network before secure communication can take place. This is called the "key distribution problem". It is a boot stamp problem; a small secret communication (over an insecure communication network) is required before any further secret communication over the network can take place. A private courier or a secure communications channel is used for the distribution of keys over the network.

Public – key cryptography solves this problem by announcing the encryption procedure E (and associated key) in the public domain. However, the decryption procedure D (and associated key) is still kept secret. The crux of public key cryptography is the fact that it is impractical to find the decryption procedure from the knowledge of the encryption procedure. This revolutionary concept was advocated by Diffie and Hellman. 17 Encryption procedure E and decryption procedure D must satisfy the following properties.

1. For every message M, D (E(M)) = M.
2. E and D can be efficiently applied on any message M.
3. The knowledge of E does not compromise security. In other words, it is impossible to derive D from E.

DIFFIE AND HELLMAN

Diffie and Hellman suggested that one way to implement public – key cryptography systems is to exploit the computational intractability of the inversion of one – way functions. [17] A function f is one – way if it is convertible and easy to compute; however, for almost all in the domain of f, it is computationally infeasible to solve equation y = f(X) for X. Thus, it is computationally infeasible to derive the inverse of f even though is known. Note that given f and output y (f=(x)) of the function, what we want is that the computation of input x should be impossible. Diffie and Hellman in produced the concept of "trapdoor one – way" functions [17] In function f is referred to as a trapdoor one – way function if the inverse of f is easy to compute provided certain private "trapdoor" information is available. An example of private "trapdoor" information is the value of the decryption key $_{kd}$. Clearly, a trapdoor one – way function f and its inverse can be used as matching encryption and decryption procedures in public – key cryptography. Various implementations of public – key cryptography which make use of such one – way functions have been proposed. Next, we discuss a popular implementation by Rivest, Shamir and Adleman.

INVEST – SHAMIR – ADLEMAN METHOD (RSA)

In the Rivest – Shamir – Adleman (RSA) method, a binary plaintext is divided into blocks, and block is represented by an integer between 0 and n – 1. This representation is necessary because the RSA method encrypts integers. The encryption key is a pair (e, n) where e is a positive integer. A message block M (which is between 0 and n – 1) is encrypted by raising it to the eth power modulo n. That is, the cipher text C corresponding to a message M is given by

$C = M^{en}$ 1 (modulo n)

Note that cipher text C is an integer between 0 and n – 1. Thus, encryption does not increase the length of a plaintext. The decryption key is a pair (d, n) where d is a positive integer. A cipher text block C is decrypted by raising it to the dth power modulo n. That is, the plaintext M corresponding to a cipher text C is given by

$M = C^{dn}$1 (modulo n)

A user X has his / her own set of encryption key (e_x, n_x) and decryption key ($d_{x,}$ n_x) where the encryption key is available in the public domain but the decryption key is secret and is known only to user X. whenever user Y wants to send a message M to user X, Y simply uses X's encryption key (e_x, n_x) to encrypt the message. When X receives the encrypted message, it decrypts it using its decryption key (d_y, n_x)

INTRUDERS

In an important early study of instruction, Anderson identified three classes of intruders.

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are

individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Generally, this requires the intruder to acquire information that should have been protected. In some cases, this information is in the form of a user password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.

Typically, a system must maintain a file that associates a password with each authorized user. If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords. The password file can be protected in one of two ways.

One – way function: The system stores only the value of function based on the user's password. When the user presents a password, the system transforms that password and compared it with the stored value. In practice, the system usually performs a one – way transformation (not reversible) in which the password is used to generate a key for the one – way function and in which a fixed – length output is produced.

Access control: Access to the password file is limited to one or a very few accounts.

If one or both of these countermeasures are in place, some effort is needed for a potential intruder to learn passwords. On the basis of a survey of the literature and interviews with a number of password crackers, the following techniques for learning passwords:

1. Try default passwords used with standard accounts that are shipped with system. Many administrators do not bother to change these defaults.
2. Exhaustively try all short passwords (those of one to three characters)
3. Try words in the system's online dictionary or a list are readily available on hacker bulletin boards.
4. Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
5. Try users' phone numbers, social security numbers, and room numbers.
6. Try all legitimate license plate numbers for this state.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

IP SECURITY

IP Security, or simply IPSec, consists of a fundamental architecture and a collection of request for comment (RFC) standards developed by the internet Engineering Task Force's (IETF's) IP Security Working Group. Naturally, IPSec is not the only standard for Internet – related security; there are several special applications – oriented efforts in the works, but IPSec is the solution when dependable, general – purpose security is needed for confidential communications via the Internet or a private IP backbone. IPSec provides three distinct forms of protection for the transfer of private data via a public or private IP network, including the Internet:

- **Authentication:** The property of knowing that the data received is the same as the date that was sent and the claimed sender is in fact the actual sender.
- **Integrity:** The property of ensuring that data is transmitted from source to destination without undetected alternation.
- **Confidentiality:** The property of communicating such that the intended recipients know what was being sent but unintended parties cannot determine what was sent.

To provide these three forms of protection, there are three basic elements in IPSec: the Authentication Header (AH): the Encapsulating Security Payload (ESP): and the Internet key Management protocol (IKMP), AH and ESP can be used separately or is combination to achieve the desired level of protection.

An Authentication Header (AH) involves a keyed code placed in the headers of all packets. As the name implies, AH authenticates the user with a "digital signature" known only to the holders of the key(s). The signature is the unique result of "hashing" the packet through a special algorithm. AH also provides data integrity because any changes, however minor, to the pay load during transmission are detected by the provide any confidentially because it does not encrypt the packet's payload. The two most popular AH standards are the Message Digest Version 5 (MD5) and the Secure Hash Algorithm Version 1 (SHA – 1). MD5 use up to a 128 – bit key: SHA -1 offers stronger protection with key lengths up to 160 bits. Standards for 96 – bit MD5 and SHA – 1 are expected soon.

The Encapsulating Security Payload Keeps transmitted information strictly confidential by fully encrypting the data, or payload in all packets. This prevention other users from "listening in" to the open exchange an information. Because only

Basic Packet

IP	DATA

Transport Model Packet

IP	AH	ESP	DATA

Original

Tunnel Mode Packet

IP	AH	ESP	IP	DATA

Tunnel **Original**

Basic Packet

Instructed users have the key(s), ESP also provides authentication and integrity. As with AH, integrity insults from a mismatch between data received and in packet's checksum – here in clear text- in the header. The dominant ESP standard is the Data Encryption Standard [DES]. DES supports key lengths up to 56 bits. Triple DES (3 DES) uses three sets of keys to encrypt, then decrypt and finally re - encrypt the payload. Which is the equivalent for using a key of up to 168 bits long. Because ESP actually encrypts all data, it introduces more "overhead" and requires more processing time than AH. Both of which can impact performances.

The benefits of IPSec include:

1. When IPSec is implemented in a firewall or router, it provides strong security that can be applet in all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security – related processing.
2. IPSec is below the transport layer (TCP, UDP), so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper layer software, including applications, is not affected.
3. IPSec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per – user basis, or revoke keying material when users leave the organization.

Applications of IPSec

The Internet community has developed application specific security mechanisms in numerous application terms, including electronic mail (Privacy Enhanced) Mail Pretty Good Privacy [PGP], network management simple network management protocol version 3[SN – MP_K – 3]. Web access (Secure HTTP, Secure Sockets Layer [SSL]), and others. However, users have some security concerns that cut across protocol layers. For example, an enterprise can run a secure, private TCP / IP network by disallowing links to untrusted sites, encrypting packets that leave the premises. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security ignorant applications.

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

1. Secure branch office connectivity over the Internet. A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
2. Secure remote access over the Internet: An end user whose system is equipped with IP Security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for travelling employees and telecommuters.
3. Establishment of extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentially and providing a key exchange mechanism.
4. Enhancement of electronic commerce security: Most efforts to date to secure electronic commerce on the Internet have relied upon securing web traffic with SSL since that is commonly found in Web

browsers and is easy to set up and run. There are new proposals that may utilize IPSec for electronic commerce.

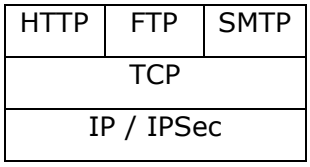
WEB SECURITY

The World Wide Web is fundamentally a client / server application running over the Internet and TCP / IP intranets. The web presents new challenges not generally appreciated in the context of computer and network security:

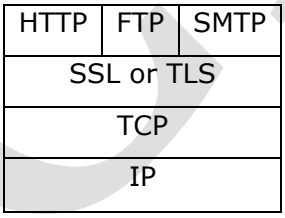
- The Internet is two way. Unlike traditional publish environments, even electronic publishing systems involving teletext, voice response, or fax – back, the web is vulnerable to attacks on the web servers over the Internet.
- The web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transactions. Reputations can be damaged and money can be lost if the web servers are subverted.
- Although web browsers are very easy to use, web servers are relatively easy to configure and manage, and web content is increasingly easy to develop, the underlying software is extraordinarily complex. This complex software may hide many potential security flaws. The short history of the web is filled with examples of new and upgraded systems, properly installed, that are vulnerable to a variety of security attacks.
- A web server can be exploited as a launching pad into the corporation's or agency's entire computer complex. Once the web server is subverted, an attacker may be able to gain access to data and systems not part of the web itself but connected to the server at the local site.
- Casual and untrained (in security matters) users are common clients for web – based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Web Traffic Security Approaches

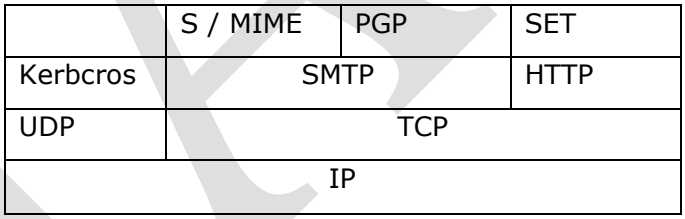
A number of approaches to providing Web security and possible. The various approaches that



(a) Network



(b) Transport level



Web Traffic Security Approaches

Have been considered are similar in the services they provide and, to some extent, in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP / IP protocol stack.

One way to provide web security is to use IP security The advantage of using IPSec is that it is transparent to end users and applications and provides a general – purpose solution. Further, IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing.

Another relatively general – purpose solution is to implement security just above TCP. The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow – on Internet standard known as Transport Layer Security (TLS). At this level, there are two implementation choices. For full generality, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications. Alternatively, SSL can be embedded in specific packages. For example, Netscape and Microsoft Explorer browsers come equipped with SSL, and most web servers have implemented the protocol.

FIREWALL

Internet connectivity is no longer optional for organizations. The informations and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial – up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the inside world to reach and interact with local network assets. This creates a threat to the organization, it enables the while impossible to equip each workstation and server on the premises network with strong security features, such a intrusion protection, this is not a practical approach. Consider a network with hundreds or even thousands of systems, running a mix of various of UNIX, plus Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. The alternative increasingly accepted, is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled by and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet – based attacks and to provide a single choke point where security and audit can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

Firewall Characteristics:

1. 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 expect via the firewall. Various configurations are possible, as explained later in this section.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this section.
3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Four general techniques that firewalls use to control a access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four.

1. **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a web or mail service.
2. Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
3. **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec
4. **Behaviour Control:** Controls how particular services are used. For example, the firewall may filter e – mail to eliminate spam, or it may enable external access to only a portion of the information on a local web server.

The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
2. A firewall provides a location for monitoring security – related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
4. A firewall can serve as the platform for IPSec. Using the tunnel mode capability described in the firewall can be used to implement virtual private networks.

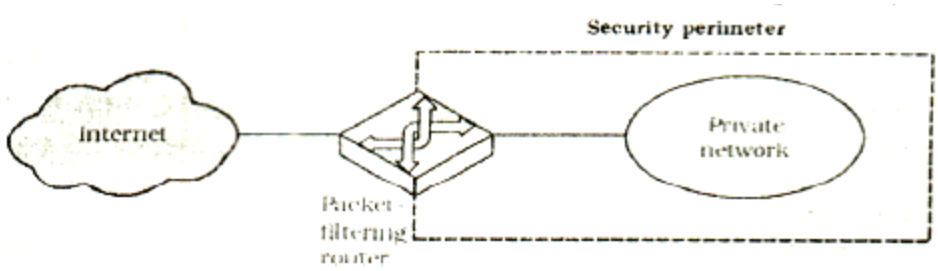
Firewalls have their limitations, including the following:

1. The firewall cannot protect against attack that bypass the firewall. Internal systems may have dial – out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial – in capability for travelling employees and telecommuters.
2. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

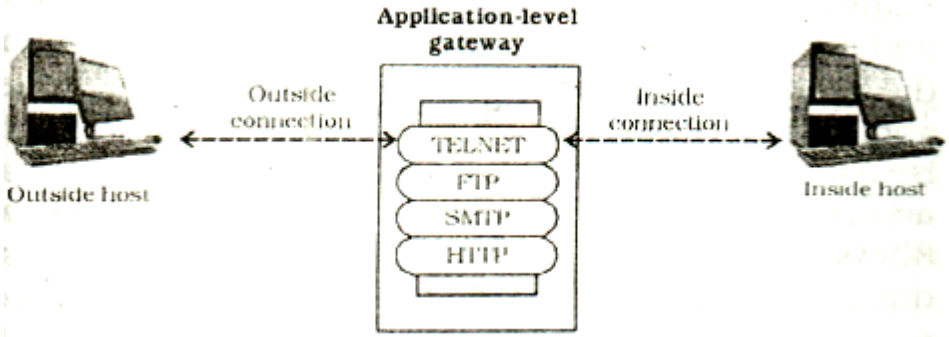
3. The firewall cannot protect against the transfer of virus – infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e – mail, and messages for viruses.

TYPES OF FIREWALL

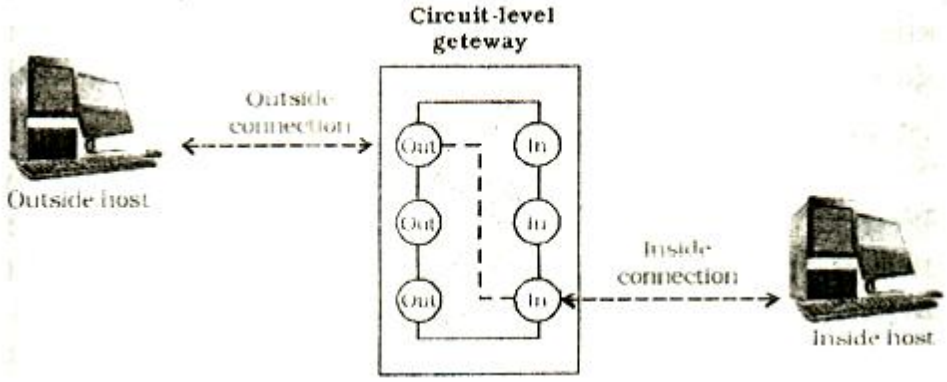
Three common types of firewalls: Packet filters, application – level gateways, and circuit – level gateways.



(a) Packet – filtering router



(b) Application – level gateway



(c) Circuit – level gateway

Packet – Filtering Router

A packet – filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP Packet (e.g., 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)

- **Source and destination transport – level address:** The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELMET
- **IP Protocol field:** Defines the transport protocol
- **Interface:** For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two defaults polices are possible:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

The default discard policy is more conservative. Initially, everything is blocked, and services must be added on a case – by – case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. The default forward policy increased ease of use for end users but provides reduced security; in security administrator must, in essence, react to each new security threat as it becomes known.

Application – Level Gateway

An application – level gateway, also called a proxy server, acts a relay of application – level traffic. The user contacts the gateway using a TCP / IP application, such as Telnet or FTP, and the gateway asks the user for two name of the remote host be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway _ be configured to support only specific features of an application that the network administrator consider acceptable while denying all other features. Application – level gateways tend to be more secure than packet filters, Rather than trying to deal with numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application – level gateway need only scrutinize a few allowable application, in addition, it is easy to long and audit all incoming traffic in both directions.

Circuit – level gateway

A third type of firewall is the circuit – level gateway. This can be a stand – alone system or it can be a specialized function performed by an application – level gateway for certain applications. A circuit – level gateway does not permit an end – to – end TCP connection; rather, the gateway sets up two TCP connections, one between in itself TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allows.

A typical use of circuit – level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application – level or proxy service on inbound connections and circuit – level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead outgoing data.

TERMINOLOGY OF MALICIOUS PROGRAMS	
Name	**Description**
Virus	Attaches itself to a program and propagates copies of itself to other program
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	Program modification that allows unauthorized access to functionality
Exploits	Code specific to a single vulnerability or set of vulnerabilities
Downloader's	Program that installs other items on a machine that is under attack, usually downloader is sent in an e - mail

Auto - rooter	Malicious hacker tools used to break into new machines remotely
Kit (Virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e – mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (Dos) attack
Key loggers	Captures keystrokes on a compromised system
Root kit	Set of hacker tools used after attacker has broken into a computer system and gained root – level access
Zombie	Program activated on an infected machine that is activated to launch attacks to other machines

NATURE OF VIRUS

A virus is a piece of software that can "infect: other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
Biological viruses are tiny scarps of genetic code eDNA or RNA that can take over the machinery of a bring cell and trick it into making thousands of flawed replicas of the original virus. Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself. The typical virus becomes embedded in a program is a computer. Then, whenever the infected computer comes into contact with an uninfected piece of software a fresh copy of the virus passes into the new program. Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network. In a network environment, the ability to action applications and system services on other computers provides a perfect culture for the spread of a virus
A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executers secretly when the host program, system. Once a virus is executing, it can perform any function, such as erasing files and programs.

- Dormant phase: The virus is idle. The virus will eventually be activated some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
- Propagation phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a surety of system events, including a count of the number of items that this copy of the virus has made copies of itself.
- Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Most viruses carry out their work in a manner that is specific to a particular operating system and, in some cases specific to a particular hardware platform. Thus, they are designed to take advantage of the details and weakness of particular systems.

TYPES OF VIRUS

There has been a continuous arms race between virus writers and writers of antivirus software since viruses first appeared. As effective countermeasures have been developed for existing types of viruses, new types have been developed. Suggest the following categories as being among the most significant types of viruses.
1. **Parasitic virus**: The traditional and still must common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed by finding other executable files to infect.
2. Memory – resident virus: Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
3. **Boot sector virus:** Infects a master book report or boot record and spreads when a system a booted from the disk containing the virus.
4. Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software.

5. Polymorphic virus: A virus that mutates with every infection, making detection by "Big- nature" of the virus impossible.

6. Metamorphic virus: As with polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their beataior as well as their appearance.

One example of a stealth virus was discussed earlier: a virus that uses compression so that the inferred program is exactly the same length as an uninfected version. Far more sophisticated techniques are possible. For example, a virus can place intercept logic in disk I / O routines, so that when there is an attempt in read suspected portions of the disk using these _____, the virus will present back the original uninfected program. Thus, stealth is not a term that applies to a virus as such but, rather, is a technique used by a virus to evade detection.

A polymorphic virus creates during replication that are functionally equivalent but have distinctly different bit patterns. As with a stealth virus, that purpose is to defeat programs that scan for viruses. In this case, the "signature" of the virus will vary with each copy. To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent instructions. A name effective approach is to use encryption. A portion of the virus, generally called a mutation engine, creates a random encryption key to encrypt the remainder of the virus. The key is stored with the virus, and the mutation engine itself is altered. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates a different random key is selected.

THE INTERNET'S HISTORY

The Beginning: A "Networks of Network"

The scales of the Internet were planted in 1969, when the advanced Research Projects Agency (ARPA) of the U.S. Department of Defense began connecting computers at different universities and defense contractors. The resulting network was called ARPANET. The goal of this early project was to create a large computer network with multiple paths – in the form of telephone lines – that could survive a nuclear attack or a natural disaster such as earthquake. If one part of the network were destroyed other parts of the network would remain functional and data could continue to flow through the surviving lines.

THE INTERNET'S MAJOR SERVICES

The internet acts as a carries for several different services, each with its own distinct features and purposes. The most commonly used Internet services are

- The World Wide Web
- Electronic Mail
- News
- File Transfer Protocol
- Chat
- Instant Messaging
- Online Services
- Peer to Peer services

To use any of these services, you need a computer that is connected to the Internet in some way. Most individual users connect their computer's modem to a telephone line (or use a high – speed connection such as DSL or a cable modem) and setup an account with an internet service provider (ISP), a company that provides local or regional access to the Internet backbone.

UNDERSTANDING THE WORLD WIDE WEB

The World Wide Web (also known as the Web or WWW) was created in 1989 at the European particle physics Laboratory in Geneva, Switzerland, as a method for incorporating footnotes, figures, and cross references into online documents. The Web's creators wanted to create a simple way to access any document that was stored on a network, without having to search through indexed or directories of files, and without having to a manually copy documents from one computer to another before viewing them, To do this, they established a way to "link" documents that were stored in different locations on a single computer, or on different computers on a network.

The collection of Documents and their links to cover the entire globe, we have a "world – wide web" of information. This concept is where the web gets its name.

Many people believe that the web and the Internet are the same thing, but this is nor correct. In fact, they are two different things. The web is a service (a system for accessing documents) that is supported by the Internet (a gigantic network)

HOW THE WEB WORKS

Web documents can be linked together because they are created in a format known as hypertext. Hypertext systems provide an easy way to manage larger collections of data, which can include text files, pictures, sounds, movies, and more. In a hypertext system, when you view a document on your computer's screen, you also can access all the data that might be linked to it.

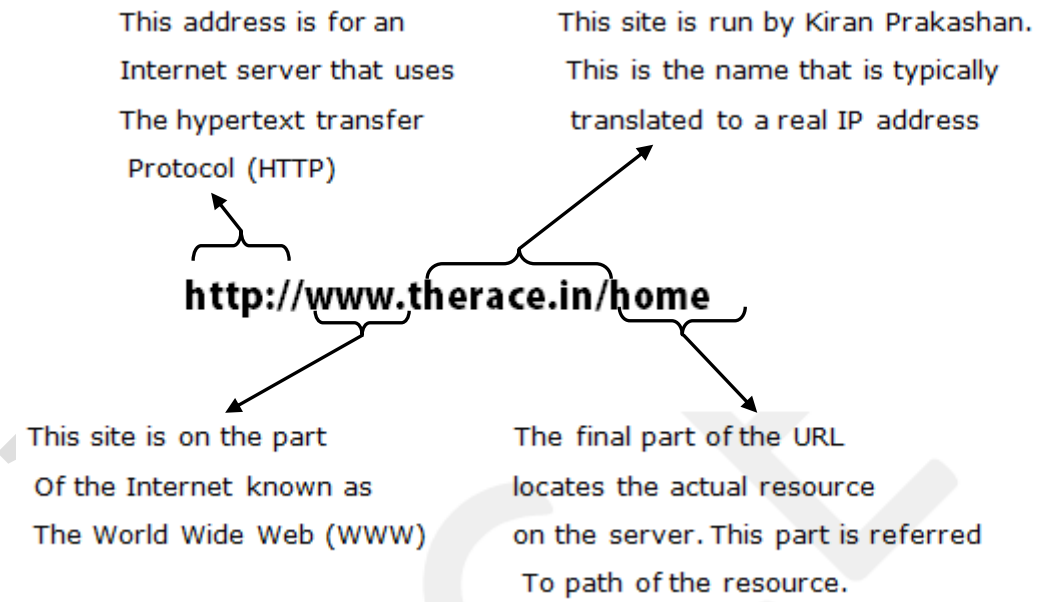
To support hypertext documents, the web uses a special protocols called the hypertext markup language or coded file that uses the hypertext markup language, or HTML. This language allows a document's author to embed hypertext links – also called hyperlinks or just links – in the document. HTTP and hypertext links are the foundations of the World Wide Web. As you a read a hypertext document – more commonly called a Web page. A collections of related web pages is called publishing the page but the process also called Posting or Uploading

USING HYPERLINKS

A hyperlink is simply a part of the web page that is linked to a URL. A hyperlink can appear as text, an image, or a navigational tool such as a button or an arrow. You can click a hyperlink and "jump" from your present location to the URL specified by the hyperlink. Hyperlinked text usually looks different from normal text in a web page: it is often under linked, but can be formatted in any number of ways. When your mouse pointer touches hyperlinked text, the hyperlinks' URL appears in the browser's status bar, and the pointer changes shape to resemble a hand with a pointing index finger.

SEARCHING THE WEB

Directories: A directory enables you to search for information by selecting categories of subject matter. The directory separates subjects into general categories (such as "companies"), which are broken into increasingly specific subcategories (such as "companies – construction – contractors – builders and designers") After you select a category or subcategory, the directory displays a list of Web sites that proved content related to that subject. The Kiran Prakashan directory at http: // www. Kiranprakashan.com



Search Engines: A search engine lets you search for information by typing one or more words. The engines then displays a list of web pages that contain information related to words. (This is type of look – up is called a keyword search. Any search engine lets you conduct a search based on a single word. Most also let you search for multiple words, such as "search AND printer", Many search engines accept "plain English" phrases or questions as the basis for your search, such as "banks books of Kiran Prakashan" or "SSC" books of Kiran Prakashan".

UNDERSTANDING E - MAIL

The most common way to create, send, and receive e – mail is by using an e – mail program (also called an e – mail client) and an Internet Connection through an ISP or LAN. There are many web – based e – mail services that allow you to send and receive e – mail by using your web browser.

E – Mail Addresses

If you have an account with an ISP or if you are a user on a corporate or school LAN, then you can establish an e – mail address. This unique address enables other users to send messages to you and enables you to send messages to others.

You can set up an e – mail account by creating a unique user name for yourself, which identifies your postal mailbox on the internet. If your name is John Simth, for example, your user name might be "jsmith" or "john_ smith". In an e – mail address, the user name usually appears before the ISP host computer's name, The user name and the host computer's name are separated by the @ symbol (commonly called the "at" symbol). So, if your ISP is America Online (AOL), your e – mail address might look like this:

jsmith@aol.com

You read this address as "J smith at a – o - l dot com".

E – MAIL AND GROUPWARE

There are various ways to communicate through the Internet. Some of them require both the sender and the receiver to be online, such as groupware while others, such as e – mail do not employ such restrictions and the sender can send data even if the receiver is offline.

E – Mail

An e – mail address is divided into two parts, namely the username and the mail server name. The two parts are separated by the symbol @. The structure of an e – mail address is as follows:

username@mailservername.com

For example, kiranpraskashan@hotmail.com is an e – mail address where,

Kiranprakashan = the username

Hotmail = the name of the mail server

.com = a commercial website

Though e – mail is a very popular service of the Internet because of its numerous advantages, it has few advantages also. The advantages and disadvantages e – mail are as follows:

ADVANTAGES

- It is a very fast medium of communication. The messages can be sent in no time irrespective of the distance.
- It is a very economic medium of communication. You are only charged the cost of being online whenever you are sending it overseas or down the road.
- Any form of data, such as text, graphics, sound, or video, can be sent throng e – mails.
- It is a secure medium of communication, that is, no one can access anybody's e – mail account without knowing the password.

DISADVANTAGES

- A slight error in the e – mail address of the recipient is enough to prevent the delivery of the message and even when you do everything right, there is always a chance of failure in one of the links between you and your recipient.
- Sometimes, viruses can enter your system through the attachments received in e – mails

CREATING AN E – MAIL ACCOUNT

The steps for creating an e – mail account are as follows:

1. Start Internet Explorer.
2. Type the address of any e – mail service provider. For example, www.gmail.com in the address bar and press the **Enter** key. The home page of Gmail appears that allows the new users to create their mail accounts and the existing users to log on to their accountants.

- Click their create an account button. The Create an account web page appears that asks for certain details like First name, Last name, Desired Login name, password, etc.
- Fill up all the necessary details in the given text boxes.
- Read the Terms of Service and click on the **I accept. Create my account** button.

A web page showing the confirmation of your account creation appears. Now, you can receive and send e – mails.

THREATS TO USERS

Networks and the Internet have created limitless possibilities for people to work, communicate, learn, buy and sell, play games, and interact with others around the world. These possibilities come from the openness of networks – especially the Internet, which is available to virtually everyone, for virtually any kind of use. However, the very openness that makes the Internet so valuable also has made it a conduit for many types of threats.

IDENTIFY THEFT

Identity (ID) theft occurs when someone impersonates you by using your name, Social Security number or other personal information to obtain documents or credit in your name. with the right information, an identity thief can virtually "become" the victim, obtaining a driver's licenses, bank accounts, mortgages, and other items in the victim's name.

Identity thieves can use several methods – low – tech as well as high – tech – to obtain the information they need:

- **Shoulder surfing:** A trick known as shoulder surfing is as simple as watching someone enter personal identification information for a private transaction, such as an AIM machine.
- **Snagging:** In the right setting, a thief can try snagging information by listening in on a telephone extension, through a wiretap, or over a cubicle wall while the victim gives credit card or other personal information to a legitimate agent.
- **Dumpster Diving:** Other techniques are as simple as stealing low – tech approach is dumpster diving. Thieves can go through garbage, cans, dumpsters, or trash bins to obtain cancelled checks, credit card statements, or bank account information that someone has carelessly thrown out.
- **Social Engineering:** In social engineering, the ID thief tricks victims into providing critical information under the pretext of something legitimate. The thief can call an unwary victim for example; claim to be system administrator at the web site of the victim's bank; and ask for the victim's user ID and password for a system check.
- **High – Tech Methods:** Sophisticated ID thieves can get information using a computer and Internet connection. For instance, Trojan horses can be planted on a system or a person's identify may be snagged from unsecured Internet sites.

LOSS OF PRIVACY

Many of the companies you deal with every day – from your local supermarket to your insurance company – maintain databases filled with information about you. You might except these firms to know your name and address, bur you might be surprised to learn that they know how many times each month you put gas in your car or buy a magazine. And a lot of companies do not keep this information confidential; they may sell it to other companies who are interested in knowing about you.

Personal Information is a business commodity that supports a huge shadow industry called data mining. Data mining is a business – intelligence gathering process that every large organization, from banks to grocery stores, employees to shift through computerized data. Companies spot useful patterns in overall behavior to target individuals for special treatment. Data mining is a $200 – million a year industry, and it is growing rapidly because it pays big dividends.

ONLINE SPYING TOOLS

Software developers have created a number of ways to track your activities online. Although many of these tools were created for benign purposes – such as helping legitimate webmasters determine who visit their sites most often – they are also being used in ways must consumers do not appreciate.

COOKIES

A cookie is a small text file that a web servers asks your browser to place on your computer. The cookie contains informations that identifies your computer (its IP address), you (your user name or e – mail address), and information about your visit to the web site. If you set up an account at a web site such as an e – commerce site, the cookie will contain information about your account making it easy for the server to find and manage your account whenever you visit.

Despite their helpful purpose, cookies are now considered a significant threat to privacy. This is because they can be used to store and report many types of information. For example a cookie can store a list of all the sites you visit.

WEB BUGS

A Web bug is a small GIF – Format image file that can be embedded in a web page or an HTML format email message. A web bug can be as small as a single pixel in size and can easily be hidden anywhere in an HTML document.

SPYWARE

The term spyware is used to refer to many different kinds of software that can track a computer user's activities and report them to someone else. There are now countless varieties of spyware, because Internet advertising is a common source of spyware.

Spyware can record individual keywords, web pages e – mail address, personal information and other types of data. This means that any number of companies can be using spyware to track your online activities. For this reason, anti – spyware development has exploded, with dozens of spyware killing products on the market.

THREATS TO HARDWARE

Threats to your computer's hardware involve incidents that have an effect on the operation or maintenance of the computer. They range from such routine things as system breakdown and misuse to malicious actions of individuals including theft and vandalism for the equipment. Disasters such as fire and flood are also threats.

POWER – RELATED THREATS

Power problems affect computers in two ways:

- **Power fluctuations** when the strength of your electrical service rises or falls, can cause component failures.
- **Power failure** when power is lost altogether, causes systems to shut down.

As the countermeasure against power – related problems, you can equip your system with one of the following devices.

- Surge suppressors protect against voltage spikes. These inexpensive plugs can be bought in most hardware stores.
- Line conditioners provide additional functions. Not only do they protect against spikes, but they also safeguard against the line noise from high demand electrical equipment operated near your computer. This protects the computer against voltage drops, called sags.
- Uninterruptible power supplies (UPS) are essentially a battery backup for your computer. A UPS protects the system from electrical events including a total loss of power. One important function of a UPS is the 'soft landing' feature. It ensures that the computer will be shut down normally if the device's battery runs out before power is restored.

CYBERCRIME

Computer crime is aimed at stealing the computer, damaging information, or stealing information. The use of a computer to carry out any conventional criminal act, such as fraud, is called cybercrime and is a growing menace. Cybercrime is growing so rapidly, in fact, that the federal government has created a handful of agencies to deal with computer – related crime. Criminal actions included setting up fraudulent bank websites to steal account information from unsuspecting customers, auction fraud, and no delivery of merchandise.

HACKING

Hacking remains the most common form of cybercrime, and it continues to grow in popularity. A hacker is someone who uses a computer and network or Internet connection to intrude into another computer or system to perform an illegal act. This may amount to simple trespassing or acts that corrupt, destroy, or change data.

In another form, hacking can be the basis for a distributed dental of service (DDOS) attack, in which a hacker hides malicious code on the PCs of many unsuspecting victims. This code may enable the hacker to take over the infected PCs, or simply use them to send requests to a web server. If the hacker controls enough PCs, and can get them to send enough requests to the targeted web server, the server essentially becomes jammed with requests and stops functioning. Today, hackers activities are usually categorized by their intent.

- Recreation attacks
- Business or financial attacks
- Intelligence attacks
- Grudge and military attacks
- Terrorist attacks

COMMON HACKING METHODS

Hackers use a variety of methods to break into computer systems. These methods fall into three broad categories.

- Sniffing: The term sniffing refers to finding a user's password There are three ways to sniff a password: password capture. Password sharing is the most common and occurs when a victim simply discloses his or her password to hacker. Password and shared out of simple ignorance, when victims do not realize that the password might be uses against their wishes or in ways they would never intend. Password guessing is done exactly as the term implies; word guessing is done exactly as the term implies; a hacker tries to guess a user's password and keeps trying until her or she gets it right. Users can safeguard against password guessing by using complex passwords. Network administrators can prevent guessing by limiting the number of attempts anyone can make to log into the network. In password capture, a password is obtained by some type of malware program is obtained by some type of malware program and forwarded to the hacker. Passwords may be captured electronically if they are sent as text that is not encrypted. For example, during a login session, a hacker may intercept the password data when it is sent to a server even if it is encrypted within the system itself.
- Social Engineering: Social engineering use to be called "running a confidence game". Another form of social engineering is the "phone survey", the application". And the "emergency situation". In these situations, a hacker may contact potential victims by phone or e – mail, and

ask the victim to provided password information for apparently legitimate reason. This method is sometime referred to as phishing.

- **Spoofing:** Hackers may alter an e – mail header to make in appear that a request for information originated from another address. This is called spoofing. They can gain electronic entry by pretending to be at a legitimate computer, which is called IP **spoofing.**

CYBERTERRORISM

Cyber ware fare and cyber terrorism are new forms of warfare; they attack the critical information infrastructure of the nation. The conventional goal in the case of cyber terrorism is to harm or control key computer systems, or digital controls. It is done to accomplish an indirect aim such as to disrupt a power grid or telecommunications. Typical targets are power plants, nuclear facilities, water treatment plants, and government agencies. However any site with network based monitoring and control systems is vulnerable if it is hooked to the internet.

CABLE

It is a new and fast emerging technology that establishes a temporary and on – demand connection between a computer and analog cable TV network to allow data transmission over the existing cable line. It required a special device called cable modem to modulate the data and provides access to speed ranging from 512 Kbps to 20 Mbps. It is suitable for both homes and businesses. It is economical as well as provides higher speed than dial – up and ISDN.

- **Digital subscriber line (DSL):** It is also a dedicated connection that uses the standard telephone lines to transmit and receive information digitally. A special modem and adapter card are required to allow data transmission. The speed provided by this connection ranges from 1.28 Kbps to 8 Mbps and thus, it is suitable for both homes and small business organizations. It is more expensive than ISDN but provides high speed. Moreover, it does not interfere with normal telephone use.
- **Leased line:** It is a permanent connection that uses a dedicated and high-speed telephone line rented for twenty – four hours a day and seven days a week. It is used by large – scale business to connect their geographically distant offices. A fixed monthly fee is charged based on the distance between the end points, and the speed of the circuit. It provides high – speed internet access ranging from 2.4 Kbps to 5 Mbps. Though it is very expensive, it provides the fastest Internet access.

Integrated Services Digital Network (ISDN) service

Integrated services digital network (ISDN) is a digital telephone services that simultaneously transmit voice, data and control signaling over a single telephone line, ISDN service operates on standard telephone lines but requires a special modem and phone service, which adds to the cost. An ISDN data connection can transfer data at up to 128,000 bits per second (128 Kbps).

The benefits of ISDN (beyond the faster speed compared to a dial – up connection) include being able to connect a PC, telephone, and fax machine to a single ISDN line and use them simultaneously. Many ISP's and local telephone companies that offers Internet access services support ISDN connections.

DIGITAL SUBSCRIBER LINE (DSL) SERVICES

Digital subscriber Line (DSL) service is similar to ISDN it its use of telephone network, but it uses more advance digital signal processing and algorithms to compress more signals through the telephone lines. DSL also requires changes in components of the telephone network before it can be offered in an area. Like ISDN, DSL service can provide simultaneous data, voice and fax transmissions on the same line.

DSL technologies are used for the "last mile" between the customer and a telephone company's central office. From there, the DSL traffic destined for the Internet travels over the phone company network in an internet exchange point (IXP) and onto the Internet.

Several versions of DSL services are available for home and business use. Each versions provides a different level of service, speed, bandwidth, and distance and they normally provide full – time connections. The two most common are Asynchronous DSL (ADSL) and synchronous DSL (ADSL). Other include High – data rate DSL (HDSL) and very High – data – rate DSL (VDSL). The abbreviation used to refer to DSL service in general begins with an x (xDSL), reflecting the variation of the first character in the DSL versions.

Banker's algorithm.

The Banker's algorithm is a resource allocation and deadlock avoidance algorithm developed by EdsgerDijkstra that test for safety by simulating the allocation of pre - determined maximum possible amounts of all resources, and then makes a "S – state" check to test for possible deadlock conditions for all other pending activities, before deciding whether allocation should be allowed to continue.

******* IACE *******