ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

An Overview towards the Different Types of Security Attacks

Malyadri K[1]

Application Developer Lead, SAVANTIS Solutions (Formerly Vedicsoft Solutions), NJ 08830[1]

ABSTRACT: In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Intrusion Detection System has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. A pattern matching IDS for network security has been proposed in this paper. Many network security applications rely on pattern matching to extract the threat from network traffic. The increase in network speed and traffic may make existing algorithms to become a performance bottleneck. This paper provided an overview on different types of security attacks.

KEYWORDS: attacks, DOS, security.

I. NETWORK SECURITY ATTACKS

To compromise between opening a system and lock it down so that no one can use it, is called security and any action that compromises the security is called a security attack. A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system.

Attacks can be categorized into following basic categories.

- Interruption: For using the data or resources it is necessary that they are available 24/7 for the authorized parties, when and where they need it. Attack on the availability of data is called interruption. Availability can be affected by intentional or un-intentional acts. Examples of un-intentional acts are, accidentally system crash, deletion and overwriting of data and some time due to non human factors like flood, fires and earthquakes. Whereas destruction of infrastructure due to wars, strikes and some attacks by hackers that crashes the system, such as denial of service *(DOS)* and distributed denial of service *(DDOS)* attacks are the examples of intentional acts. Protection against availability attacks includes backup andrestoration.

- Interception: The core concept is that the data should be hiding from unauthorized users. If some one who is unauthorized to see private data, can see or copy the data that can further be used in intensive active attack. Such an attack is known as attack on confidentiality. Data integrity can be accomplished by strong authentication and strict access controls, because some time authorized users may also a threat for confidentiality of data. They can obtain another person‟scredentials.

- Modification: Integrity of data deals with prevention of intentional or unintentional modification of data. Attack on integrity of data called modification. Different algorithms used for validation of data that can resist in alteration of data. Protection of data from modification is foremost concern than detection. Integrity of data could maintain at many layers of OSI systemmodel.

- Fabrication: Attack on authenticity called fabrication. Authenticity means that message is coming form the apparent source. It assures that you are who you say you are. User name and password is the most common way to achieve authentication, some other techniques are like smart cards and digitalcertificates.

Above mentioned attacks are shown in figure 1

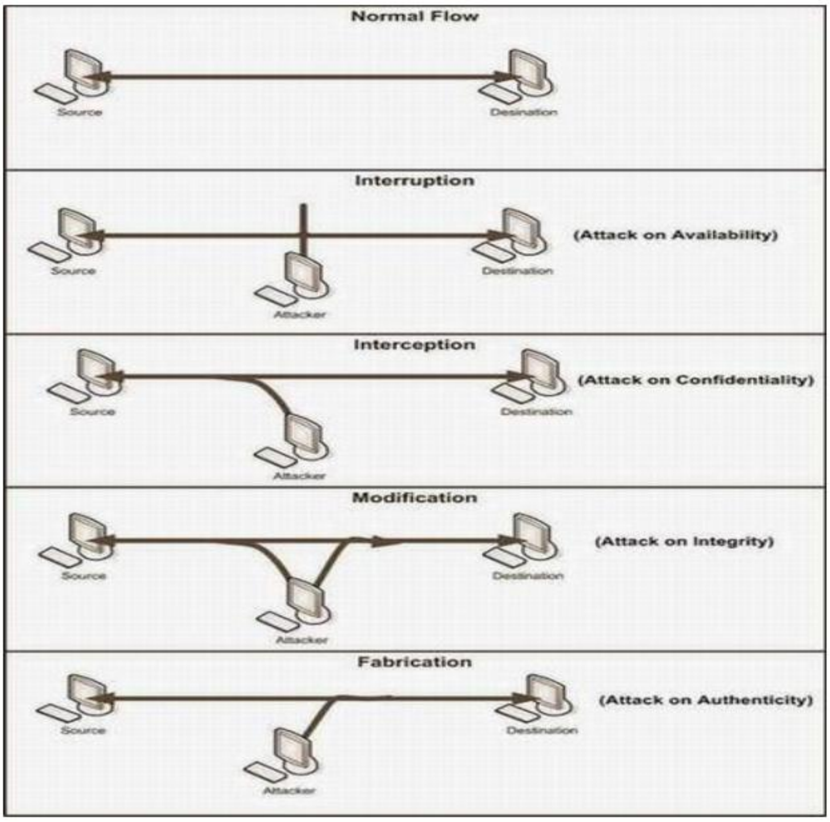


Figure 1. Basic types of Security Attacks

On the basis of these four attacks we can further classify security attacks as *passive attacks* and *active attacks*. Passive attacks are only involved in monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Two types of passive attacks are "*release of message content*" and *"traffic analysis"***.** Passive attacks arehard to detect because they do not involve in any alteration. Different encryption schemes are used to prevent against these attacks.

Active attacks are involved in modification of data (interception, modification, fabrication) or creation of false data. These attacks are further subdivided into four categories, "*masquerade", "replay", "modification of data"* and *"denial of service"*. When an unauthorized user tries to pretend as an authorized user is called masquerade attack. Replay attacks involved in capturing the message between two communication parties and replay it to one or more parties. Bring the network down to its knees by flooding the useless traffic in network is called denial of serviceattack.

Figure 2 and 3 are showing passive and active attacks.

Attacks are either active or passive. Information which hackers obtained from a passive attack is used in more aggressive active attack. We will discuss in detail some common types of network attacks.

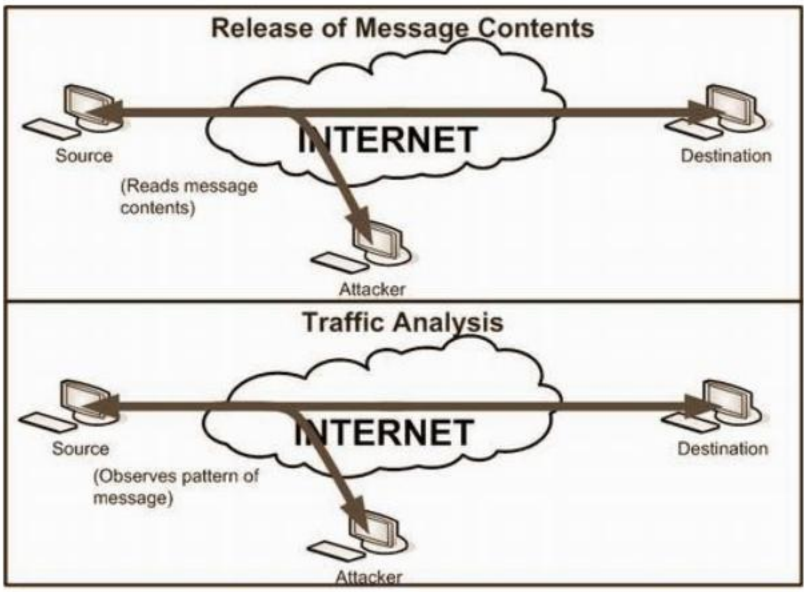


Figure 2: Passive Attacks

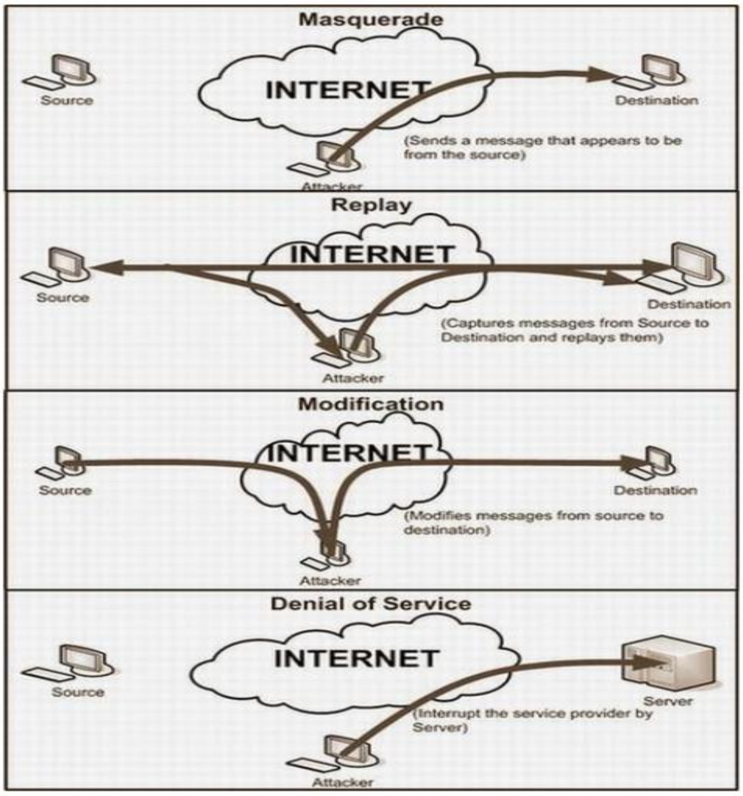

Masquerade
INTERNET
Source
Destination
(Sends a message that appears to be from the source)
Attacker
Replay
INTERNET
Source
Destination
(Captures messages from Source to Destination and replays them)
Attacker
Modification
INTERNET
Source
Destination
(Modifies messages from source to destination)
Attacker
Denial of Service
INTERNET
Source
Server
(Interrupt the service provider by Server)
Attacker

Figure 3: Active Attacks

Reconnaissance Attacks

Gathering information against a targeted host or network is called reconnaissance attack. Attacker analyze the target host and try to discover the details like alive IP addresses, open ports of the network, failour of operating system, and types of services and protocols runningon the network. Reconnaissance attacks are common they are not so much dangerous because they are not involved in any kind of alteration or destruction of data but on the other hand they show the vulnerabilities in the network. They allow hackers to see which ways are open to access the system and provide enough information to them which they can further use in denial of service (DOS)attacks.
Some basic reconnaissance attacks are: Packet Sniffers
Port scan and ping sweep
Internet information queries

Packet Sniffers

As we discussed earlier that data which is traveling across a network is not in a continuous stream of data in fact it is in the form of packets. As we know that we cannot see the atom through naked eye we need a device like electronic microscope same is in the case of analyzing the data packet. Packet sniffer is a tool or device that can be used forcapturingthepacketatdatalinklayer.Packetsnifferisnotonlyahacker‟stoolbutitcan be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. *Tcpdump*, *windump*, *wireshark (ethereal)* and *Dsiniff* are examples of different sniffingtools.

Sniffing can be of two types depending on the network.

Passive Sniffing Active Sniffing

Passive Sniffing

Passive sniffing is used in hubbed networks. The drawback of using the hub in network was that, the hub broadcast a packet to each and every machine on the network. There is a filter on each machine which decides whether to accept or discard the packet. If a packet addresses to a specific machine then filter decide to accept it otherwise discard the packet. Sniffer disables this filter so that network traffic can be analyzed.Thisstageiscalled“promiscuousmode”.Henceif„Bob‟oncomputer AsendsamessagetoJohn‟oncomputerB,asnifferoncomputerCcaneasilycapture the contents of that message even without knowing Bob and John. Passive sniffing is hard to detect because it generates no traffic on network. This type of sniffing worked well when hubs were used. To avoid passive sniffing most of the networks nowadays are using switches instead ofhubs.
Figure 4 is showing passive sniffing.

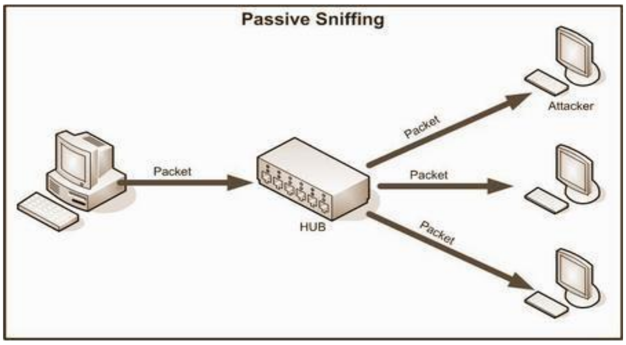


Figure 4: Passive Sniffing

Active Sniffing

Active sniffing is performed on switched network. A switch limits the sniffer to see the broadcast packets. Switch worked as a central entity, rather then broadcasting it simply get message from source machine and send it directly to the addressed machine. So if computer C is in promiscuous mode it cannot see the message form Bob to John.
It does not mean that sniffing is not possible in switched networks. Media Access Control (MAC) flooding and poisoning of the Address Resolution Protocol table (ARP) are the ways to hack a switched network.

MAC Flooding Spoofed ARP Messages

Switches worked on the basis of MAC addresses. They maintain an address resolution protocol (ARP) table in a special type of memory called Content Addressable Memory (CAM). ARP table has all the information that which IP address is mapped to which MAC address.

The act of overloading the CAM is known as MAC flooding. Low memory in older or cheaper switches can cause MAC flooding. Flooding of too many MAC addresses can fill up the memory so that switch cannot hold more entries. At this stage switch goes to a *failopen* mode and cannot perform IP to MAC mappings, starts behaving like a hub and starts transmitting the data to all machines. In MAC flooding attacker inject large amount of traffic which may draw attention towards hacker. This traffic can be detected by any sniffer detecting software.

The other technique to hack a switch network is called ARP poisoning. A review of ARP is that it is almost similar to Domain Name Server (DNS). DNS resolves domain names to IP addresses while ARP resolves IP addresses to MAC addresses. Hacker fools the switch and tries to pretend the destination machine.
He tries to convince the switch that the IP address of another trusted host belongs to him. A very interesting thing is that it is also up to the attacker that which IP address he wants to redirect to his system, spoofing thsystem, spoofing the default gateways will redirect all host messages towards the attacker. However for this, attacker has to poison host ARP table. The other way is to poison the ARP cache of a central entity of the network, hacker express that the IP address of switch (or router) is mapped with his MAC address. Through this way all the traffic first goes towards the attacker then the router. Active sniffing is shown below in figure5

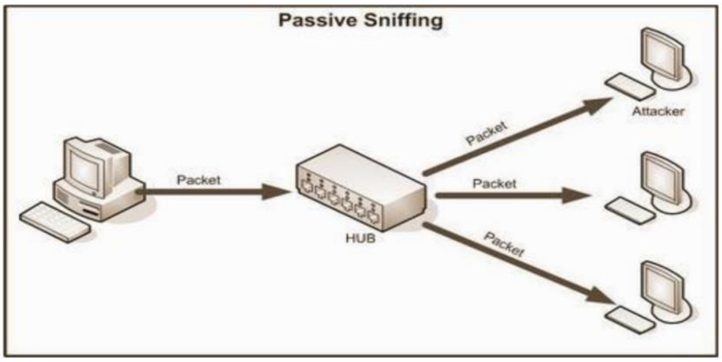
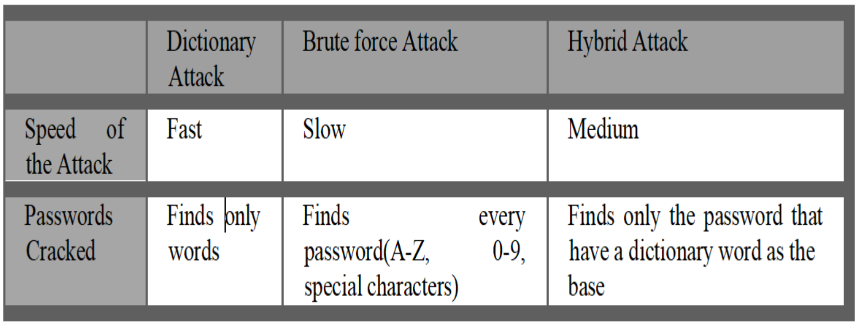


Figure 5: Active Sniffing

II. TYPES OF PASSWORDATTACK

Strong, long and encrypted passwords does not mean that they are unbreakable; it"s just a matter of time. Few years earlier the time to break a password was may be 100 days but now it"s just a matter of two or three weeks.
Different types of password cracking attacks are:
Dictionary Attack
Brute forceattack
Hybrid Attack



	Dictionary Attack	Brute force Attack	Hybrid Attack
Speed of the Attack	Fast	Slow	Medium
Passwords Cracked	Finds only words	Finds every password(A-Z, 0-9, special characters)	Finds only the password that have a dictionary word as the base

Table 1 Types of password Attacks

Different password cracking programs are available like L0phtcrack, NTSweep, NTCrack, Crack, John he Ripper etc.

Trust Exploitation

When a hacker attacks on a computer which is outside a firewall and that computer has a trust relationship with another computer which is inside the firewall, the hacker can exploit this trust relationship. We can mitigate this type of attack by using private VLANs between switches or by limiting the trust relationship between systems whichareinside and outside the firewall. We can also reduce this by eliminating useless trust relations between different servers. For example if our AAA (Authentication, Authorization, and Accounting) server is inside the DMZ (Demilitarized Zone), there is no need to have a relation of AAA server with the file server. Figure 6 explaining trust exploitation phenomena.

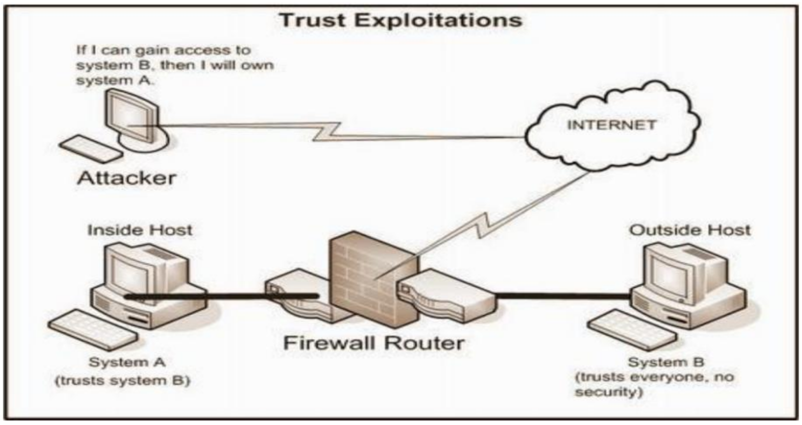

Trust Exploitations
If I can gain access to system B, then I will own system A.
Attacker
INTERNET
Inside Host
Outside Host
Firewall Router
System A (trusts system B)
System B (trusts everyone, no security)

Figure 6: Trust Exploitation Attack

PortRedirection

It is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Consider the below network in which hacker on the outside have the ability to access the public computer but not the computers which are in DMZ or which are inside the firewall. If public computer compromised by the hacker then hacker installs a software that can redirect the traffic towards the hacker, directly to the inside computers. In this way hacker makes a tunnel for communication and bypasses the security firewall. See figure 7 for port redirection attack.

Man-in-the-MiddleAttack

When hackers succeed to intrude himself between two communication parties this type of attack is called MITM (Man-in-the-Middle) attack. In this way hacker can intercept data between source and destination host, can modify data and retransmit it to the destination host and can also inject any type of false data. MITM attacks can affect on availability, confidentiality, integrity and authenticity of data. Strong cryptography can mitigate this type of attack. SSL, SSH and use of IPSec also gives end to end security (entire connection is encrypted).

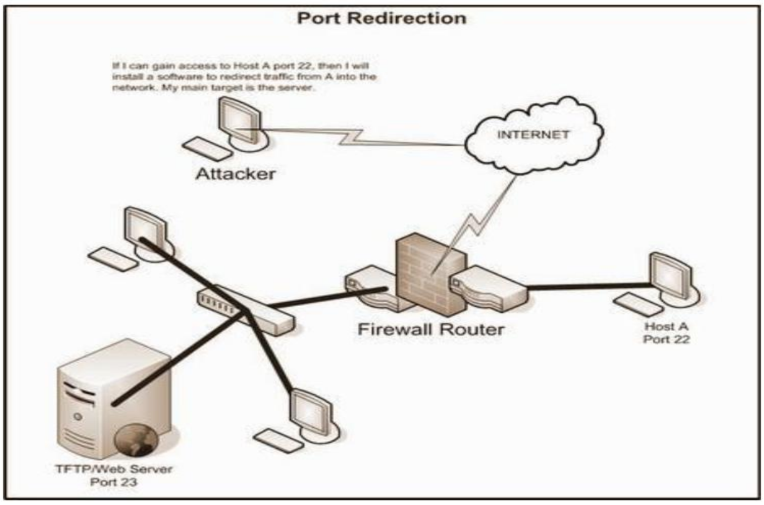

Port Redirection
If I can gain access to Host A port 22, then I will install a software to redirect traffic from A into the network. My main target is the server.
Attacker
INTERNET
Firewall Router
Host A
Port 22
TFTP/Web Server
Port 23

Figure 7: Port Redirection Attack

III. DOSATTACKS

Types of attack that bring the network down in such a way that recourses are not available even for authenticated users are known as DOS attacks. Malicious hacker saturated the target machine with useless traffic so that it cannot respond or too slow to respond and some times unavailable. Attacker may target a single machine to make it impossible for outgoing connections on the network or may attack on the whole network to make it impossible for incoming and outgoing traffic. For example attack on web site of any organization. *Ping of death, SSPing, Land, Win Nuke and SYN flood* are some of the examples of DOS attacks. In SYN flood attack hacker sends a SYN packet to target host which then respond with SYN acknowledgement, at the end attacker does not send any ACK packet to the target host that causes the connection to remain in half open state. TCP connection does not remove this connection from its table and wait to expire this session, attacker take the advantage of this and continue sending new SYN packets until TCP SYN queue filled and cannot accept new connections. The common method for blocking DOS attack is to place a filter which examines the pattern of data; if same pattern of data came frequently then filter can block thatmessage.

Distributed Denial of Service(DDOS)

In DDOS attacks several compromised systems are used to launch an attack against a targeted hostornetwork.Fortargetingahostattackerfirstcompromisesomeotherhostsonnetworkandinstall some software for controlling them usually these compromised hosts are called agents or zombies. Using these agents attacker launch overwhelm attack against the target. Compromised

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

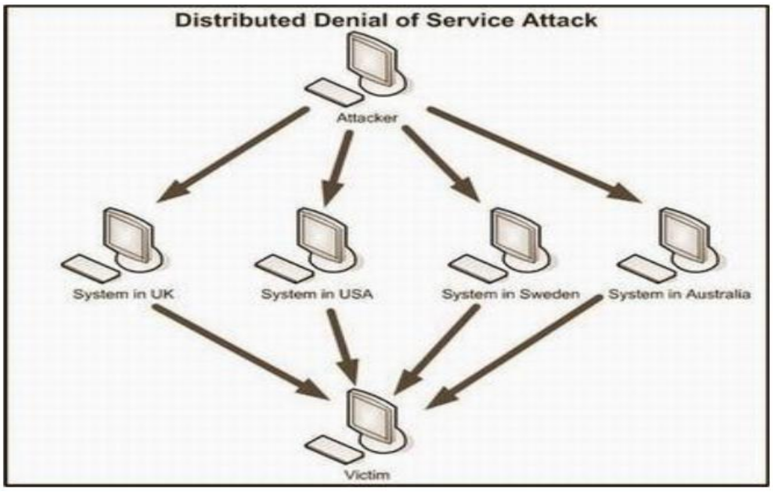


Figure 8: Distributed Denial of Service Attack

systems control with different software like *Trino and Shaft*. Example of DDOS attacks are *SMURF*, *MYDoom and TFN*. DDOS attacks are very hard to defend. To trace out the intruder is also very difficult as they are on back side and using other hosts against the victim. Figure 8 is describing distributed denial of service attack.

BufferOverflow

We can define buffer overflow as when a hacker tries to store too much data in buffer which it cannot hold. Take an example of glass which can hold 5 ounces of water if we put 8 ounces what will happen? Obviously water overflows from the edges. Buffer overflow is similar to this example;

where glass corresponds to buffer and water corresponds to data. The overall goal of this attack is toweakenthefunctionofvictim"sprogramsothathackercaneasilytakecontrolofthatprogram. Buffer overflow is the best known attack on security which can cause attack against availability, integrity and confidentiality of data. Examples are *NetMeeting Buffer overflow, Linux Buffer Overflow, Outlook Buffer Overflow.*

Viruses and Other Malicious Program

Viruses and other malicious program have the ability to make duplicate copies of them on an ever increasing number of computers. A "*Virus"* is just like a computer program that spread by copying itself into other programs. Another malicious program *"Worm"* is spread through the network. Without the network it cannot spread and can eliminate only when whole network or system is shutdown. Examples of popular worms are *Code Red, Slammer, Storm Bot.* A maliciousprogram that resides in system and execute on an event like date or time is called **"***Logic Bomb", "Trojan Horse"* is another type of malicious program that hackers use to steal useful information like user name, password and bank account codes.

IV. CONCLUSION

Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. This paper provided an overview on different types of security attacks.

REFERENCES

[1] AWhitePaper,–Securing the Intelligent Network‖, powered byIntel corporation.

[2] Network Security [Online] available:http://en.wikipedia.org/wiki/Network_security.

[3] –Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, BhavyaDaya.

[4] Ateeq Ahmad, –Type of Security Threatsandits Prevention**”,**AteeqAhmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[5] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p.257