Network Security Threats & Prevention Methodolgies - A Review

Fayyaz Masood[1], Syed Shah Muhammad[2], Sarfaraz Ahmed[3]
Department of Computer Science, Virtual University of Pakistan, Lahore
Pakistan
syed@vu.edu.pk
sawan@vu.edu.pk

Salman Qadri[4]
DCS & IT, The Islamia University of Bahawalpur
Pakistan
salman.qadri@iub.edu.pk

ABSTRACT: *There are many kinds of threats of malware like virus, worms, Trojan horse and many more. Along with external attacks internal attacks are also big security threat for any company or enterprise. Today's world is very dangerous for network browsing and surfing without safety measures.*

To overcome these threats, there are some security measures like encryption, antivirus programs etc. Although a lot of work has been done in this field and still work is continue against network security threats yet attackers and hackers are becoming powerful day by day. In this paper I have discusses all these issue, I have also point out some points for future researchers in the field of network security.

Keywords: Network Security, Virus, Trojan, Security Threat, Malware

Received: 3 July 2016, Revised 12 August 2016, Accepted 19 August 2016

1. Introduction

Network security plays an important role for the safety of the data travelling in the network. Browsing and surfing can be very harmful for any user or organization without safety measures. There are many kinds of malicious program over the internet which can harm our computer or data. Attackers and hackers use new types of malicious programs; if one attack fails they attack with new weapons. On the other hand our safety measures are not so affective to stops all kinds of attack over the network. There are many kinds of security threats like internal as well as external threats. In this paper I have tried to describe

all of them. I have also tried to describe some safety measure and there mechanism. I have tried to find the best way while travelling over the network.

In the final section of this research paper I have analyzed and conclude my opinion, I have also point out some future direction of research for new comers.

2. Threats and their Types

When there is a chance or circumstances that may break the security measures this is called threat. The threat may be internal (within the organization) or external threat (outside the organization) networking threats

2.1 Internal threats

These are the types of threats which an organization faces by its employees and EX-employees. These employees and EX-employees can be very dangerous for the organization because they know all the internal system of the organization; they also know the weaknesses and holes within the organization. So an organization should be very careful about them. Companies and organizations have to trust on these employees to run the business properly. Some greedy employees can't see progressing a company or organization so they behave in different manner due to their greedy nature.

A major type of security threat is from IT employees. These employees can be very fatal for the company. IT deportment in an organization is the backbone of the organization and they are the system developer also. They completely know all the weaknesses of the security system so it is very easy for them to launch an attack on company or use some other mechanism which can cause a great loss for the company.

The term employee sabotage is used when these IT employees cause the destruction of hardware and software of the system. They can also launch time bomb or logic bomb on the company's computers.

These employees can be dangerous because they have full knowledge of the security system of the company or organization. They wait for a suitable chance and when they find some holes in the system they may do their work which is unauthorized to them.

Employee Hacking is another kind of security threat, this means that an employee access the part of the system resources which are not authorized to him. This hacking is done without the knowledge of the company or organization.

An employee can steals the system resources of the company or he can steal other costly things of the organization like furniture, money or some secret business information and later on he can sell this important information to other company which can cause great damage to the parent company. This is also called employee financial theft.

Some employees download sexual data from the internet and waste the company time and money for personal interest.

There is another kind of employees who download data from the internet more than that data which is allowed to download. This is another kind of theft which can cause company a great loss.

Another kind of employee financial theft is theft of intellectual property (IP). The term intellectual property is very important for any company; it contains the business plans, security measures, customers list etc. the leakage of intellectual property (IP) of the company can cause a great loss for the company because this information can be used by another company to defeat first company goals.

Temporary workers are also a great risk for any well growing company. A company has to trust on these temporary workers to run the business and to create the atmosphere of friendship among the workers. After completing the task these temporary workers have to leave the company so they can create different kinds of threat for the company. They can steal important data, business plans and other secret information from the company and sell this information to other company.

EX-employees of the company are another major danger for the company. They create different kinds of threats for the company because they have left the job. So they have no tension of termination the jobs.

With the passage of time these types of employee and EX-employee are increasing day by day. As the result of these frauds a company can bear financial loss, reputational damage etc.

2.2 External Threats

External attacks are launched from outside the organization. There are many kinds of external attack some of them are given below:

2.2.1 Denial of Service attack (DoS)

Denial of Service attacks (DoS) are originated from online gaming service. In denial of service attacks the victim computer or website is bombard with many request of service. These requests are beyond the capacity of requests the website can handle. So the website or victim computer can't handle the large number of requests and stops or slow down its services.

Denials of Service attacks (DoS) are becoming more and more dangerous for network security. Some denials of Service attacks (DoS) are launched in the form of UDP Flooding and Intermittent Flooding.

Today's denials of service attacks are very dangerous. These attacks are completed in two phases. The following diagram illustrated the DoS attack.

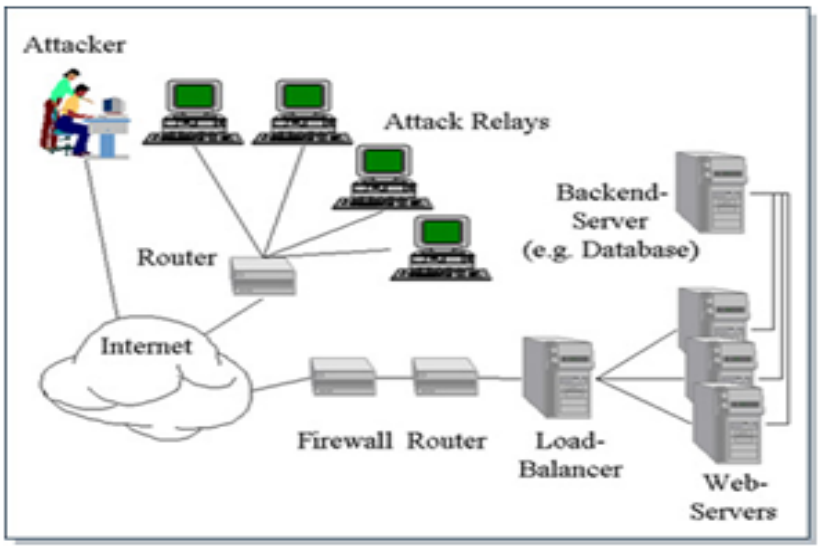

Figure 1. DOS Attack

In the first phase the attacker or programmer prepare many compromised computers for the attacks; these compromised computers are also called bots. In the second phase of attack the attacker bombard the victim computer or website with its companion computers called bots. The victim computer or website can't bear the large number of requests and slows down its services or collapses.

2.2.2 Man in the middle attack

Man in the middle attack is another type of external network security threat. This attack is launched for session hijacking. If two persons are communicating over the network the attacker may launched its attack on client computer and steal it IP and pretends itself as a client and after modifying the data sends it to the other side, the attacker can silently watch the whole session and can pick the required information he needed.

Stealing IP address and claiming itself as a client is also called IP Spoofing. If there is mechanism of authentication between the either side (client and server) then this type of attack can be minimized. In this type of attack two parties are communicating with each other believing that there is no one between them although there is a middle man present who listens both of them and alter the communication if he wants.

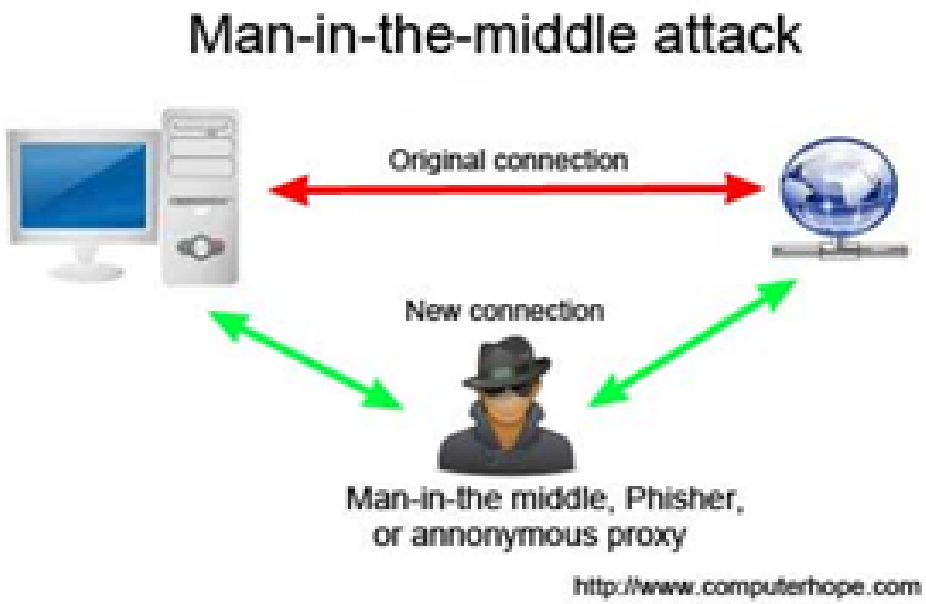

Figure 2. Human involvement in the Attack

2.2.3 IP address Spoofing

In this type of attack the attacker use the false IP address to access the network or pretends that it is the valid IP address , when he accesses the network or the victim computer he can change , damage or redirect the data to hacker's computer or some other direction.

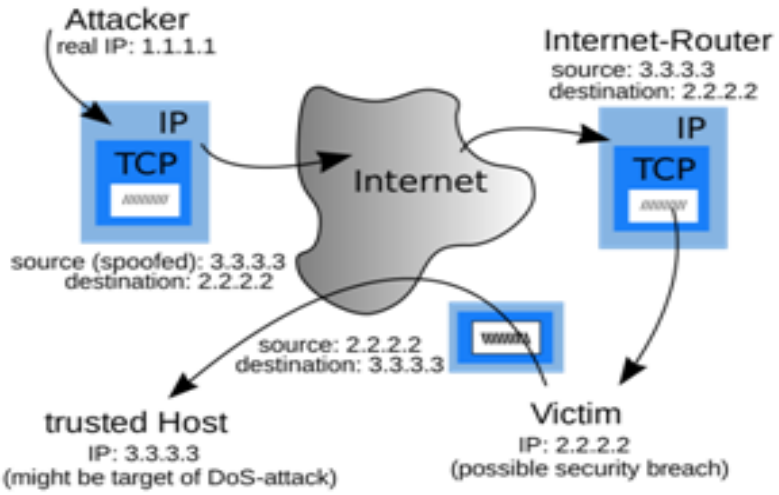

Figure 3. IP Address Spoofing

2.2.4 Compromised Key attack

In Compromised Key attack the attacker somehow obtain the secret key of the encrypted data. Although it is very difficult task for the attacker to obtain the secret key because there are many encrypted algorithms involve there yet if the attacker succeed to access the secret key, then he can decrypts the data and can get plaintext data, the attacker can also alter the data and even delete the data without the involvement of sender and receiver. This stolen secret key is also called compromised key.

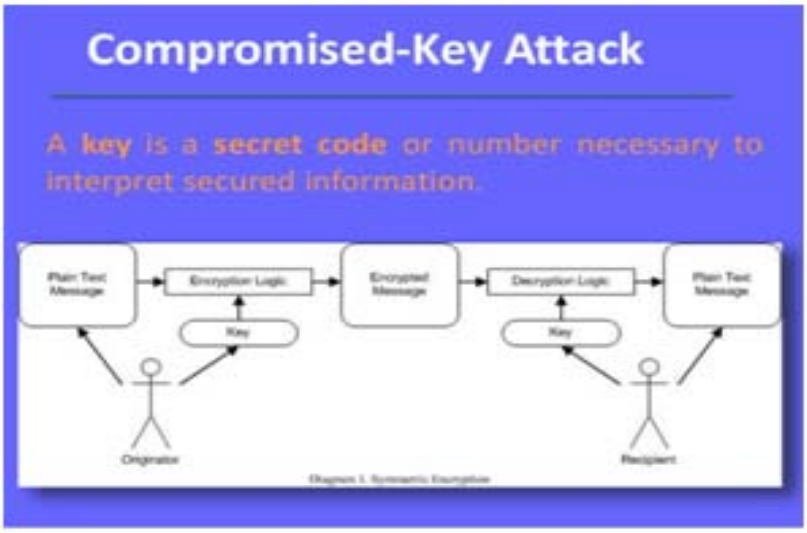

Figure 4. Compromised Key Attack

2.2.5 Sniffer attack

In this type of attack the attacker use a special software program called sniffer , the sniffer can do many things over the internet for example a sniffer can read the data travelling over the internet, a sniffer has the ability to break into data packet and can read all the secret information. The sniffer can corrupt the accessed data or alter it.

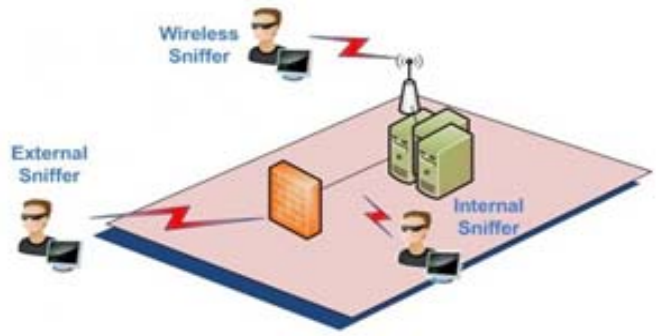

Figure 5. Sniffer Attack

2.3 Application layer attack

This is another type of network attack; in these types of attacks the attacker targets the application program on the server. The attacker uses a mechanism which can create bugs or problem on server. If an attacker succeeds in doing so then he can create many problems for the network or the server itself. The attacker can delete accessed application or he can put a virus in the application, he can even collapse the whole operating system, the attacker can put a sniffer on the network to access the network traffic. This is actually very alarming situation for the network administrator.

2.3.1 Trojan Horse

In the world of computer science Trojan horse is very familiar for the user of computer. The Trojan shows itself as a healer program but inside that program there can be virus which can cause many problems for the user.

The Trojan does not work like a virus, it has no ability to republic ate itself but it can be very dangerous for the victim computer. Some Trojan Horses have the ability to delete system file and they pretend as if they are system file. Trojan horse has the ability to put virus on the host computer. Actually this is very dangerous type of malicious program which can harm

our computer data or application.

Figure 6. Trojan

Another kind of Trojan horse called downloader is also very dangerous for the network user. This is an apparently small downloadable program, when the user click on it to download it starts downloading even more bigger program (Trojan horse) which can be very harmful for the victim or host computer.

2.3.2 Rootkits

This is another dangerous program which can take hold the administrator of the computer and can damage or hijack it recourses. These programs have the ability to hide themselves from malware detection devices. There is a big reason for not detecting Rootkits malware because every Rootkits detector program can detect the specific Rootkit for which it is made to detect it. That's why it is very difficult and sometime impossible for the antivirus program to detect or remove it from the computer.

2.3.3 Virus

A very common type of computer malicious program is virus. A virus is an executable computer program it has the ability to attach itself to host application program. Now a day every network administrator is busy to clean his network from virus. As we know virus is an executable program so every executable program has a risk of virus. Virus is spread when the host object executes. After this virus looks for any other object which can work itself as a carrier , after searching a carrier virus attach itself to carrier and in this way virus spread from one file to another. Virus has also ability to attach itself with movable media like floppy discs, USB drives, CD's and many other such devices.

2.3.4 Worms

This is another type of malicious program. It is different from the virus in a way that it is an independent program; it does not need any carrier program to transfer from one place to another place.

A worm has an advantage over virus that it has the capability and mechanism which makes it easier for the worm to use the network services, so by using these services worm has the ability to spread more rapidly as compare to virus. Majority of the worms spread by email facility. Usually worms use network to transmit copies of original code to other computers present on the network.

Another kind of worms is direct propagation worms; they have very fast and active spreading nature. They have the ability to jump from one computer to another in the fraction of seconds. It spread so rapidly that we can't do any safety measure.

2.3.5 Logic Bomb

This is another type of virus; it also works like a virus it is executed on a specific time or by doing specific action. After executing, logic bombs work and spread like a virus and Trojan horses.

Some hacker blackmails the organization or other focal person to pay money if they avoid the dangerous result of logic bomb.

When we talk about the time bomb the only difference between logic bomb and time bomb is that the time bomb execute only on specific time or day, we have an example of time bomb which is also called Jerusalem virus which execute every Friday the 13^{th}, on that day it delete all the infected files or folder present on the victim computer.

2.3.6 Spyware

One of the most common types of malicious program that can be very harmful for the victim computer. These types of programs stealthily gather information on the victim computer and send this information to the hacker or attacker. Another kind of spyware called camera spyware has the ability to turn on your camera without your prior permission. Spyware can also do same action with the microphone.

Another type of spyware called keystroke logger. This is also very dangerous program present on host computer. It has the ability to store all the keys pressed by the user on its memory later on the keystroke logger sent this sensitive data to the hacker of the program. In this way keystroke logger can steal our password and other secret information.

One of the most amazing and surprising type of spyware informs the user that he/she has been logged out of the session, he/she needs to login again. Actually this is fake information given by the spyware to trap user password. Now if the user acts upon the advice given by the spyware, the spyware steal the user password and sends it to the hacker of the program.

Another kind of spyware called data mining spyware works like the keystroke logger spyware. It searches for the data present on the hard disk of the victim computer. After searching the value able data present on the hard disk, data mining spyware sends this information to the hacker of the program.

3. Social Engineering

This is another technique that is used by the attacker to convince the user to do such act which goes in favor of the attacker. Some simple user can easily be trapped by such environment which is provided by the attacker.

In social Engineering a malware program is presented before the user in such an attractive way that user can't refrain itself from pressing clicking the button. If the user does so, a virus or malicious program present behind the button download automatically this can harm the victim computer.

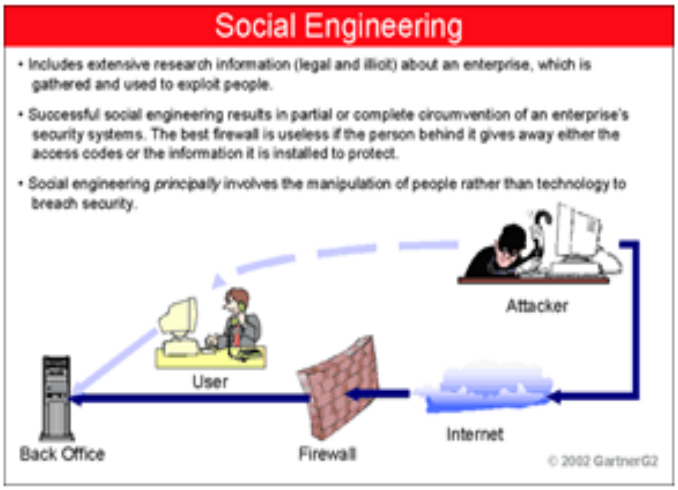

Figure 7. Social Engineering

This is threat environment. It is very difficult to escape from these threats while travelling over the network without any safety measure. Although the above discussed mattes do not covers whole of the threat environment but a common user faces these kinks of threats on the network.

We can escape from the dangerous results of these threats if we adopt some safety measure while travelling over the network. These safety measures provide us a shield from network security threats.

The network security measures can be of many types. This security measure can be technical, human or mixture of both of them.

4. Safety Measures

Now we discuss about the safety measures against these threats. First of all we discuss the security measure against the internal threats:

1. Safety measure against internal threats.

Internal security threats are very difficult to stop because it is not possible for an organization to check the entire staff member; anyhow there are some rules that make it easier for any organization to minimize the chance of fraud.

- While appointing the staff an organization should appoint honest, hardworking and well reputed person.
- The organization should adopt a strong policy against any fraud case.
- It is clear to anyone that there will be zero tolerance policy against any fraud.
- There should be strict check and balance over the workers of an organization.
- The criminal record of any person should be checked before appointment.
- There should be fraud prevention check in the organization, it may include CIFAS Staff.

If an organization adopts these safety measures it is believed that committing of fraud by staff will minimized. It is also duty of organization that honest and hardworking staff should not affect by these strict policies. An organization should encourage any honest worker if he sees any evidence of fraud and tells the responsible persons of organization.

4.1.1 Safety Measures Against External Attack

While travelling over the network our data is not secure if we have not adopted any safety measures against malware programs present over the network. We can avoid external attack if we have proper antivirus system on our machine. This antivirus program should be updated.

To avoid external network security attack we should use some encryption schemes. These encryption schemes provide our data a layer of protection against all network security attacks. These network security schemes are of two types which are Symmetric Key Encryption and Asymmetric Key Encryption schemes. We also have combination of both schemes which are called Hybrid Encryption Schemes.

These data encryption schemes provide us data authentication, authorization, integrity of data, confidentiality and service of nonrepudiation.

If we have the threat of spoofing attach then there should be a strong mechanism which check data authentication, here we don't use our security password in plaintext section, there should be a Secure Sockets Layer (SSL). This layer provides our data security against cookies' abuse.

If we have fear of tampering of data over the network then we should have a strong authorization mechanism to avoid this danger, along with this we should use strong hashing algorithm, and the use of digital signature will guarantee that our data will not be tempered over the network.

Some time some person denies that he/she did not send data, in this case we have a mechanism of digital signature which guarantee that a person can't denies if he/she send any data.

If we want to stop the danger of sniffing attack we should encrypt our data completely and enforce authentication service on both sides.

Denial of service attack is big danger for any organization or website, although it is very difficult to stop these kinds of attack yet we can minimize the risk of attack if we develop TCP/IP protocol in such a way that it is very harder for the attacker to break that layer, we should have a mechanism to decrease the connection establish period we can minimize the denial of service attack to zero level if there is a mechanism that ensure that connection queue will not be worn out.

Password cracking is another network threat that can be very dangerous for the security of data. We should always use strong and long password which cannot be broken by any attacker or hacker. If our password length is small there is more chance of stealing password over the network. Long password can increase the work of attacker or password cracker to break the password.

Despite of all the security measure taken by us against the network security threats it is alarming fact that attacks on the network are increasing day by day. Having all encryption schemes and antivirus programs, we are unable to stop all the attack on the network. All these security measure do not guarantee that our network is safe from attack.

It is need of the time to create such an effective and everlasting security scheme that minimize the ever growing attacks on network security. Although we are successful in many fields of network security yet there are some malicious programs which are still challenge for our security measures.

5. Discussion

Now a days we are living in the threat environment, in this threat environment we have to face many challenges while travelling over the network. This is threat environment. It is very difficult to escape from these threats while travelling over the network without any safety measure. Although the above discussed mattes do not covers whole of the threat environment but a common user faces these kinks of threats on the network.

We can escape from the dangerous results of these threats if we adopt some safety measure while travelling over the network. These safety measures provide us a shield from network security threats.

To minimize these security threats we have to adopt many safety measures for the safety of our data and network. The network security measures can be of many types. These security measures can be technical, human or mixture of technical and human.

These threats can be internal and external. Internal security threats are within the organization and an organization can face many problems due to these internal threats. It is very difficult to overcome these internal threats because a company or an organization has to trust on its workers to keep the business running. Anyhow these internal threats can be minimized if a company or organization takes some safety measure before appointment of the workers.

On the other hand external security threats are very common over the network. These threats can be launched the attacker or hacker. These threats are of different kinds. Like man in the middle attack, password stealing, session hijacking, sniffing and spoofing. Another major kind of external security threat is denial of service attack.

We have different safety measures to overcome these threats. For example we have a variety of utility and antivirus programs. While travelling over the network we use many encryption schemes to protect our data from attackers and hackers.

As it mentioned above we use many antivirus program to safe our computer from malicious programs and while sending our data over the network we use many encryption schemes but after doing all this, our network is not secure so far. While browsing website on the internet we may have virus attack or any Trojan horse can enter into our system without our information. This is not a secure environment, this is not the environment for which we are struggling and wasting our time and money on it. We should have to adopt some new mechanism to overcome the abuse of network attacks and we should also create some strong antivirus programs which should have the ability to change their behavior dynamically according to the nature of the virus or any other malicious program.

We should try to program new encryption scheme which are so strong that it is impossible for any attacker or hacker to breach

our security mechanism.

But this is the imaginary world I am talking. So far we have no such mechanism to adopt so we should take care while searching on the internet or while sending our data over the network. We should use available anti malicious programs so efficiently that there is no chance of virus attack on our system.

6. Conclusion

After studying all threats of network security environment I would like to conclude that our network is not secure so far, we are spending our time and money for the security of our network but hackers and attackers are also spending much more energy and resources to find the way to breach our network and they are successful in many fields. Although our network security measures are very efficient and strong yet there are many gaps and holes between them. I am not saying that our whole network is not secure, surly it is secure but it should be 100% secure rather than 60, 70 or 80%.

If we are using wireless network then we should always use network security key. The administrator should not remain login after completing his task. He should logout immediately.

In a small network environment we should run antivirus program on each computer of the network to keep the virus out of the network and machines. If we want to share internet connection we should always use router to avoid the attack of hackers.

The most important thing is to keep our computer up to date so that our antivirus program may remain active against advance malicious program.

7. Future Research Directions

Although this paper covers many of the security issue of the network yet there are many weaknesses and holes in the entire security security system. It is need of the hour that we focus on advance research on algorithms which can provide the solution of many challenges we are facing so far, we should review or security protocols, architecture, policies and implementations.

Today's most challenging network threats are Denial of Service Attack (DoS) and Distributed Denial of Service Attack (DDoS). These threats are open challenge for the researchers and programmers. It is need of the hour to accept these challenges and try to overcome the threats faced by network users.

References

[1] Kartalopoulos, S. V. (2008). Differentiating Data Security and Network Security, Communications, 2008. ICC '08. IEEE International Conference on, p.14691473, 1923 May.

[2] Xu, W., Trappe, W., Zhang, Y., Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. Proceeding of ACM Mobihoc, 46-57. ACM Press, New York.

[3] Dowd, P.W., McHenry, J.T. (1998). Network security: it's time to take it seriously, Computer, 31 (9) 24,28, Sep.

[4] SecurityOverview, www.redhat.com/docs/manuals/enterprise/RHEL4 securityguide/chsgsov.html

[5] Molva, R. (1999). Institut Eurecom, Internet Security Architecture, *Computer Networks & ISDN Systems Journal*, vol. 31, p. 787804, April.

[6] Aad, I., Hubaux, J.P., Knightly, E. (2004). Denial of service resilience in ad hoc networks. Proceedings of ACM Mobicom. ACM Press, New York.

[7] Yaar, A., Perrig, A., Song, D. (2003). Pi: a path identification mechanism to defend against DoS attacks. Proceedings of IEEE Symposium on Security and Privacy.

[8] Aether Wire Location, Corp., Low-Power, Miniature, Distributed Position Location and Communication Devices Using Ultra-Wideband, Nonsinusoidal Communication Technology, AEther Wire Location, Corp., Semi-Annual Technical Report, ARPA Contract J-FBI-94-058, July 1995.

[9] Barrett, M., Little, M., Poylisher, A., Gaughan, M., Tardif, A. (1998). Intelligent Agents for Vulnerability Assessment of Computer Networks, *In*: Proceedings of the ARL Federated Laboratory 2nd Annual Symposium,

[10] Blundo, C., de Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M. Perfectly-secure key distribution for dynamic conferences, *In*: Advances in Cryptology: Proceedings of Crypto92, E. F. Brickell, ed., LNCS 740, Springer-Verlag (1992), 471–486.

[11] Imielinski, T., Badrinath, B.R., Freebersyer, J. (1998). Project Summary: Dataman Project – Information Services for Low-Powered Wireless-Mobile Clients, DARPA ATO Sponsored Research, Rutgers University.

[12] Govindan, R., Faber, T., Heidemann, J., Estrin, D. (1999). Ad-hoc Smart Environments, *In*: Proceedings of the DARPA/NIST Workshop on Smart Environments, Atlanta, June.

[13] Mills, D. Low Energy Communications and Routing for Microsensor Networks, *In*: Proceedings of the ARL Federated Laboratory 4th Annual Symposium, 21-23 March 2000, College Park, MD.

[14] Menezes, A., Oorschot, P., Vanstone, S., (1997). “Handbook of Applied Cryptography”, CRC Press, New York