Volume 2, No. 4, July-August 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Emerging Techniques for Securing Modern Computer Networks

Hammad Khalid*
Department of Software Engineering
Faculty of Engineering and IT, FUIEMS
Rawalpindi, Pakistan
hammad_khalid_3223@yahoo.com

M. Aqeel Iqbal
Department of Software Engineering
Faculty of Engineering and IT, FUIEMS
Rawalpindi, Pakistan
maqeeliqbal@hotmail.com

M. Usman Shabbir
Department of Software Engineering
Faculty of Engineering and IT, FUIEMS
Rawalpindi, Pakistan
ushabbir_89@yahoo.com,

Umer Farooq
Department of Software Engineering
Faculty of Engineering and IT, FUIEMS
Rawalpindi, Pakistan
umer_ms13@yahoo.com

Abstract **–** Networks mostly seem as organizational architecture appropriate for supporting organizational clients to learn and equally built innovative conveyance. Our journal appertains to various types of Network Security Attacks and the ways in which they can be avoided and reduced. Network security has become one of the most critical areas of research. Cryptography plays an important role in Network Security. It converts readable data into unreadable data so that the communication between two clients can be private and the third party cannot conscious of this data. Since, the current era of computing is demanding the highest level of computational security. Since, last few decades a variety of algorithms and structures have been demonstrated to manage the issue of Network Security but still this is not the end of the world. There are many issues relevant to Network Security which is still irresolvable. We will discuss the kinds of network security attacks that hackers perform to harm and steal data from unauthorized means and to prevent such attacks which tools are best and reliable. We expect that the reader will have an immense broad view on security in generic, and conceive how to reduce and manage risk personally at home and in the workplace.

Keywords **–** Network Security, DDoS, Trojans, Cryptography

I. NETWORK SECURITY

Computer networking is association of computers undergoing independent and sovereign computing. The computer in a network follow certain protocol adopting which communication is under gone between computers of a network. Study of mode of evaluation of security requirements and needs of such systems and inferable design, implementation and deployment is the initial scope of the Network Security [1].

Security in network terminology refers securing the information being transmitted on a network.

Risk is the measure of loss or an unwanted event. Risk in network security terminology refers to the chances of breach into information being sent across a network. The information security is one of the major concerns in the network's architecture designing. Being unaware to threat and non adaptation to security measures is for sure unacceptable in any network especially in the current technological era. [2], [3].

In the present era of technology the threat are becoming more and more effective and are generating mass damage due to acquisition of latest technology. The use of latest and more effective technology in the networking attacks had made many security measures to become worthless in front of them and they could easily be breached. The mentioned scenario requires more effective steps to be taken in order to be secure from the threats and eliminate any risk chances [3].

Generally risk in network security perspective compromises of three general factors that if simultaneously active yield threat to a system as shown in figure 5. The factors include the following: - [4] (figure 1)

A. Vulnerability
B. Threat
C. Criticality

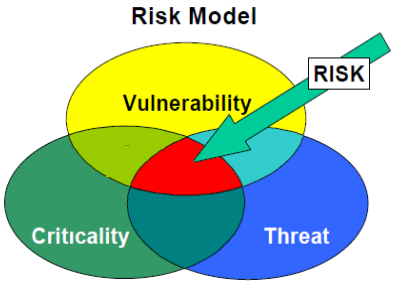

Figure 1: Risk Model

Vulnerability is defined as methodology of attacking that are possible by the virtue of which asset could be exploited or compromised. Criticality is the priority for a

network attacker to breach network for getting certain information. Third influential element is that of the threat which refers presence of such network intruders elements who intend approaching or attacking a network. Risk occurs when all the features are simultaneously present. Table 1 shows the amount of damage that could be yielding due to different network security lapses [4].

Table-1: Threat Frequencies and Damage

Sources of Information Systems Security/Usage Problems	Nature of the Threat	Probable Damage	Frequency *
Maliciousness (disgruntled employee or agent provocateur)	• Capability to Inflict Damage or Destroy, Compromise Intelligence • Enhances Potential for Outside Attacks • Deliberate Intent	Substantial	Unknown
Disdain of Security Practices Carelessness Ignorance	• Capability to Inflict Damage • Enhances Potential for Outside Attacks • Unintentional	Unknown	Unknown

Cryptography is specified by converting of information into scrambled code that are decoded and sent over a public or private network. For the cryptography encrypts the data into 2 forms, symmetrical (Secret Key) and asymmetrical (Public Key). Symmetric encryptions use the same principal in order to undergo encryption same procedure is adopted as that for decryption. Such encryption can be defined in different names like secret, shared, and private keys. The encryption principal can be loosely related to the decryption key. Plain text also yields attacks on symmetric cryptography and they are hack able and at occasion easy to decode. Professional programming and operations of the cryptographic methodologies can minimize such threats. As shown in Fig .1.

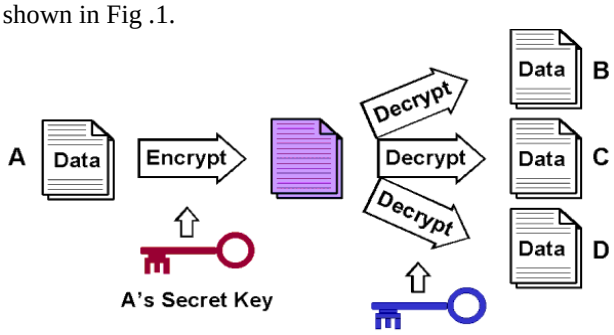

Figure. 2: Encryption vs Decryption

Different principles are implemented in Asymmetric cryptography for undergoing encryption and decryption. The data is encoded adopting principles of following public and private key principals each of which are inaccessible from one other. As shown in Fig .2.

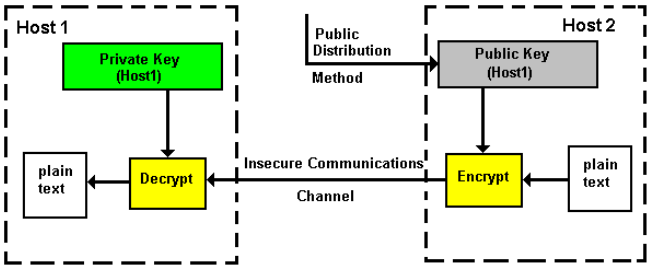

Figure.3: Encryption vs Decryption

There are various kinds of Network Attacks that hackers are performing these days, some have become old, some are still being used and some are being modified so that they can cause data leakage and different functions like that [1], [2].

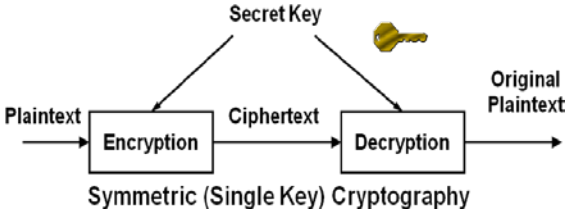

Figure 4: Symmetric Cryptography

The main network security attack that can be performed through email is to use email as a carrier through which worms and Trojans can be carried into the very heart of your network. Once these Worms/Trojans are carried into your network, they can perform different tasks assigned to them like they can sit quietly and send information to the attacker without notifying the victim. Whereas, some Worms/Trojans stick to the heart of the network and damage it e.g. network performance might be reduced or your private and confidential information can be leaked or accessed by hackers via unauthorized means. The percentages of different type of Trojans that are spread these days are shown in Fig .3.

The other major attack that is being performed on the networks is Denial of Service. Any system or network on the wild internet can be attacked via DoS. The intention of a DoS attack is to impart your systems ineffectual for the duration of the attack. This attack can be either performed by an individual person, a group or a community. If a single person is performing DoS attack on certain network then it won't do much as compared to a group or community performing same task on the same network. As shown in Fig 1.4. Now-a-days, groups of hackers perform these attacks on servers, this attack results in server down and due to this attack the websites cannot be accessed that are hosted on that server. It is to be kept in mind that this attack can only be performed on the broadband with high speed.

A dial-up user cannot perform this attack. The other part of DoS attack is Distributed Denial-of-Service. This is the kind of attack in which more than one attackers attack on the same machine net resulting denial of service for the clients on that machine. An intruder starts a DDoS attack by taking advantage of vulnerability in parent system. Infiltrator from the system identifies and communicates with other systems that can be compromised. The infiltrator piles the cracking tools available on the Internet on multiple or sometimes thousands of exposed systems. Through a single command the attacker instructs the controlled systems to launch many flood attacks against a specified target. The flood of packets to the target causes a denial of service [4].

The other type of attack that intruder instructs is to get unauthorized access to the remote system. Either the attacker wants full, admin or root access or either he wants partial control of the system. This happens due to bad passwords that mostly owners choose. They make easy passwords and use the same passwords on different places.

This results in exposure to their systems. If your password is encrypted, it won't last long and will get decrypted by the attacker in a second. There are many crackers on internet that crack there encrypted passwords. Brute forcer does the same work. To avoid such thing, always choose difficult passwords, insert numbers and special characters into your passwords so it won't be easy to crack [3], [4].

The other attack that mostly hackers perform is send worms & Trojans to the victim. It installs itself on the remote pc and stays there for as long as it can. These Worms/Trojans will perform whatever task they are given by the attacker. These worms and Trojans are also called as malicious programs. The chance of getting effected by it is through many means. You can get affected by opening websites. There are some websites that are Unauthorized and there are worms and Trojans on them, when you open that website, they will install themselves into your pc and then stick to it. The other mean is through email. Hackers send victims infected emails. There are these programs on internet called as mailer; they have to capacity to send thousands of mails at a time. The hackers just need to add the mailing list and then he attacks. To avoid such attacks, download antivirus, there are many antivirus on the internet that watch your computer for threats and other malicious programs. Install them and regularly update them. And install a firewall in your system. These two softwares will block any malicious program trying to enter your system and thus your system will remain protected from threats [4].

The main problem is to stop these network attacks and if they are unstoppable then try to avoid them. We have to stop and avoid Worms and Trojan. Trojans are not viruses they are actually malware that are hidden in exe files. You can get Trojans in your pc from many ways, like you downloaded any exe file from an email or you downloaded an exe file that looked like something else that you were looking for or you clicked on any "Click Here!!" link on the website, this will result in dropping Trojans in your pc. Sometimes, you install an Antivirus and scan all your drives including registries etc your Antivirus might detect these Trojans and might not be able to remove them. At this stage the real problem arises. If you are not able to remove them, then there many ways to remove them, some include like installing any anti-malware software that will most probably remove the Trojan, if not removed in this case then install/Activate Firewall, this will surely remove any Trojan if present. Firewalls are more persuasive against Trojan works; they won't allow the Trojans to work on victim pc.

One other form of malware is Worm. It also works as Trojans. It contains an executable script. They occasionally spread with Internet chat, peer-to peer and many other ways. Chances are that while you are downloading a file from an email attachment u might get affected by worms. Once it is installed in pc, it itself generates random email messages and attaches worms with them and sends them spontaneously. This might result in opening of TCP ports and flood the LAN with Denial of service. They usually spread very fast indeed and get undetectable by Antivirus because the updates might not be added to the database. They might install one or several files on your pc and they might rename them as system files which might get difficult to remove. It changes the registries also. The safe and effective way of removing a Worm is by using dedicated removal tools. The problem that occurs mostly in removing a worm is that it is active so files are in use and cannot be deleted [4].

The other problem is of DDos attack. Attackers might infect many pc and then control them in the form of "Botnets" and may launch a flood of coordinated Distributed Denial of Service attack or they can use this for Cyber attacks. Some hosts don't even know whether they are under attack or not unless they view there logs for untoward network life. Following problems might arise when you are experiencing DDos attacks.

a. Machine show high CPU load,
b. Complaints from clients about slow/or no site access.
c. Services fail at high rate and affect business.
d. Slow running of programs.

To avoid such attacks take the following measures,

a. Install a Firewall on your host/server.
b. Use applications that might detect/alert you when the attacker is trying to pass the gateway/hosts and break-in attempts.

There is no software for preventing DDos attacks, the only way to stay safe is avoid such attacks, implement effective security measures and keep a regular check up on the server/host.

II. EVALUATIONS AND RESULTS

We have evaluated that there are many ways in which network threats are affecting its security. We have also bumped upon some ways in which they can be removed or avoided. The first thing that should be kept in mind for network security is to make safe and secure passwords, make passwords difficult, use capital letters and also use special characters. If you want your password to be more secure then encrypt them. Use any encrypted which is available on internet, or ask any developer to develop it for you. Now-a-days, mostly passwords are encrypted in form of hashes. The hashes most commonly used are Md5, SHA1, and CRC32. They are also difficult to decrypt. These hashes are also sub categories of Cryptography. They work under Cryptography. As we know that encryption is the way of encrypting data and then decrypting it when the receiver receives it. If a hacker somehow manages to get a password that is hashed and if it is difficult to decrypt this password then it will be garbage for him e.g. if we have a password like "hRj13aS_@47", after decrypting it in Md5 hash, we will get our hashed password like "b596deee58760f009af5de24816ade24".

The other thing we have evaluated about is Worms and Trojans and how they can effect network security and how to remove them and or avoid them. Trojans and Worms are silent killers. They don't much mess up with your system are worst security killers. They steal your information and sensitive data and send it to the attacker. They use your pc to send virus to other pc and hence can affect thousands of pc in matter of weeks. This might also reflex your reputation in front of you mates or teachers. What if they download an infected file from your email or through peer-to-peer

connection, they will get infected and they will blame you for doing this activity. So the most convincing way is to avoid it and secure you from these threats. Don't download unnecessary files or those files which are trustworthy. And try avoiding opening sites which are entrusted because they might be Trojan/Worm affected and might infect your pc/network. I recommend you to use Mozilla Firefox because it blocks those sites which are infected by Trojans/Worms [5].

The last worst thing that we evaluated is the DDos attack on Networks/Servers/Hosts. Bypassing it is very challenging. There is no software or any application to avoid it or get rid of it. There are only certain steps that need to be acquired to avoid such attacks. There are some servers that are DDos free but they are expensive but once you purchase them you can get rid of this tension. DDos attack can be performed on either a single person, or a website/server or organization. Those steps which need to be taken are already described above [6].

III. APPLICATION AREAS

A. Trojans:

Networks security tools are vastly being used now-a-days. According to inspection supervised by Bit Defender [Antivirus Company] from January to June in 2009, the malware that is on the rise is "Trojan", 83% of the world is affected by Trojan malware [4], [5].

B. Botnets:

Past few years, people used to showoff and make money by developing a virus and then sending in to an individual victim. But now-a-days, people are using Botnets, it is the procedure of gaining access of victim's pc and the attacker can do whatever he wants. He can either make money with these botnets or use it for revenge purposes. These botnets computers can range from thousands to millions. The attacker can send thousands of spam emails in short time [5], [6].

C. Phishing:

The other method that the attacker uses mostly alternate to hacking software's is phishing. They use social engineering in this process. They fool you by making you trust on them. After some conversation you think that they can be trusted so they take advantage of this time and scam you right away. Now-a-days, hackers mostly use phishing pages to get passwords. They send you an email claiming that it is from Bank or an EBay etc, and after you open that page you enter your real information and you don't even know that it is being logged. The passwords are sent to the hacker and then you are redirected to some other page [5], [6].

D. IP spoofing:

This is the method in which the hacker attacks the target victim by communicating with him with the IP that belongs to the victim. The computer thinks that it is talking to itself and this result in OS crash.

E. DNS poisoning:

This is the type of attack in which hacker sends false DNS information. This might result in diversion of the traffic and the victims might not be able to reach there web server and the attacker might get the chance to get the confidential information from the victims.

F. Sniffer Attack:

A sniffer is an application or a device that allows the attacker to capture and monitor data packets sent over network. If the packets that are being sent over network are encrypted then it will be difficult for the attacker to decrypt them otherwise if they are not encrypted then the attacker gain read the communication done between client and server. Attacker can also cause damage to the server by using this technique [6].

G. ICMP Attack:

It is the type of attack which doesn't require authentication. It redirects message and causes the host to switch gateways which gives the attacker the advantage to sniff the packets being sent. ICMP destinations are unreachable and can cause the host to drop connection. ICMP gets request/reply by sending echo commands.

H. Ping Flood:

Such an attack is meant to make a server overloaded and eventually it gets down. It could be easily done by opening dos prompt and then executing <Server IP> -t command that will initiate pinging. This command makes server busy and eventually the server is down.

I. Simple Dos Attack:

In this scheme the attacker's identity is blocked by spoofing technique. Such attacks could be easily blocked. As shown in Fig .6 [7], [8].

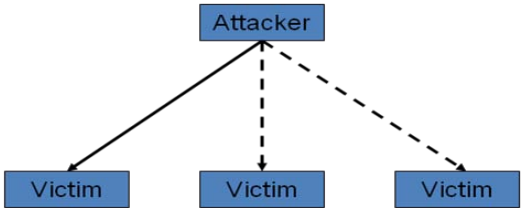

Figure .5: Simple Dos Attack

J. Coordinated Dos Attack:

In this type of attack the first attacker attacks a different victim to cover up the real attack. In this case also the attacker spoofs the source to hide origin. This is harder to stop as compared to simple Dos attack. As shown in Fig .5 [8].

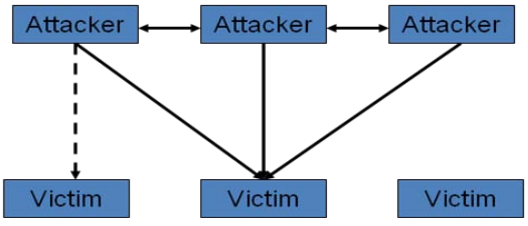

Figure .6: Coordinated Dos Attack

K. Distributed Dos Attack:

In this type of attack the handlers are usually very high volume servers and it becomes easy to hide attack packets. In this case the attackers are mostly home DSL users. In this case it is very difficult to track the attacker down. Some people call DDos attack also as flash crowd. Flash crowd is like many clients using a service legitimately. Generally the flash crowd disappears when the network is flooded. And sources in flash crowd are clustered.

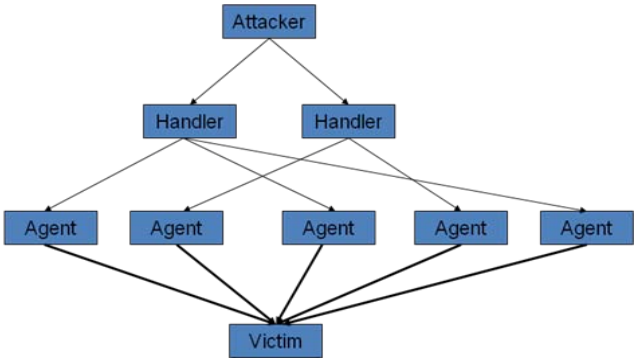

Figure .7: Distributed Dos Attack

L. Firewalls:

Mostly people that get attack are due to not installing/activating there firewalls. Lots of vulnerabilities on hosts are in networks. Users usually don't keep there systems up to date. And there are lots of patches available for there OS and if patches are not available then attackers usually use exploits. To prevent this type of attack always limit access to the network and put firewalls across the perimeter of the network. These firewalls block the unusual activity that is trying to act on pc. Firewall ask administrator for his approval even if he is installing a program or an application.

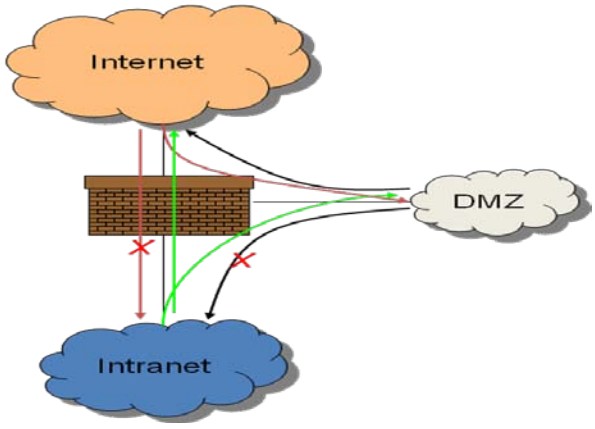

Figure .8: Fire wall

IV. GENERAL ALGORITHM

The data along being transferred along a network also needs certain security measures that need to be assured along with data transfer. The security of critical data of organizations is of immense importance and so curtail is its security. There are large numbers of different data transmission protocols defined that ensure the reliable transfer of data along a network. The network design along with ensuring the data transfer along a network also needs to ensure the basic CIA principles. The CIA refers to confidentiality, integrity and availability of data being transmitted. Confidentiality refers ensured no unauthorized access to the information, integrity refers to the trustworthiness of the data resource ensuring no data is changed from its original form whether accidently or willingly and availability refer the data availability when required.

Among the secure data transfer protocol is the internet protocol security commonly referred as IPSec. In the IPSec protocol the host and the receivers IPs are encapsulated and the actual segment is merged into another segment bearing a proxy or fake IP address. Figure shows the merging of Segment being transferred into a segment bearing fake IP address [6], [8].

As a result if one intends intercepting the sent information it needs the IP of host and receiver that is hidden in this case. Figure shows document map of IPSec protocol. The IPSec protocol used numerous techniques of file encryption such as DES 3DESand AES and file hashing techniques such as MPS, SHAI etc.

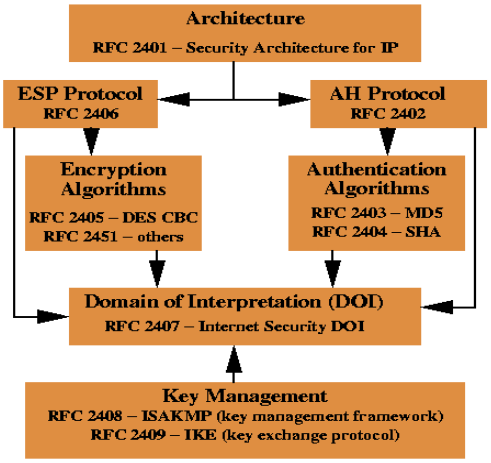

Figure.9 IPSec Document Map

V. POTENTIAL RESEARCH AREAS

A lot of research is being done in Network Security now-a-days. The network security program emphasizes to secure a network. There is a lot of research being done to avoid getting hacked and leak confidential information [8], [9]. Programmers now-a-days, test different operating systems and find many patches in them. These patches are then sent to OS Company to remove such mistakes and vulnerability in upcoming versions. Whereas some programmers leak these patches and these patches are seen by hackers which take a advantage of this bug and they hack the persons computer. Those people who are using newer version are secure from these attacks. Whereas the people who are using older versions, are in danger and they can be hacked anytime [9].

If patches are not found then programmers do find exploits and these exploits are sold to hackers in good price.

These exploits are then used by hackers in wrong manner. These exploits after getting old become useless but same is the case above for users using older versions.

Attackers usually attack those sites easily which are not configured accurately by admin or programmer. This may involve mistakes done by programmer/webmaster in networks. Inexperienced programmers/webmasters usually do this kind of mistakes. So research is being done in this case also so that the programmer who is new in his profession should be able to minimize the mistakes done by him [7].

Past few years, hackers used to use brute force attacks on networks and other sites. Brute force is like trying each password from a wordlist of thousands of words on certain network. It has end now-a-days, because many network administrators have placed a CAPTCHA on there login pages, this is an image which contains letters written on them which are to be typed to securely login with correct info. This CAPTCHA can only be filled by human being because computer can not understand what is written on it. Some network administrator's don't use this technique which results in leaking of there passwords by getting a brute force attack [10].

The next attack that hackers mostly use is social engineering. This is a way in which people fool administrators, users etc. Hackers make friendly relations with the victim and ask questions in such a manner that the victims easily answer those questions and after he is hacked he comes to know that he himself gave the password to the hacker. As we know that in password recovery mode most time we have to enter a security question and answer too so that if in case we forget the password then we can answer the security question and recover the pass again. For example if question is like "What was your first pet name?" Hackers take advantage of this and while talking to victim asks random questions and then change there display picture to an animal picture. In most cases victim himself starts the topic on pets, but if he doesn't then you have to take the initiative and start the topic and in random questions ask him about his first pets name, believe me he himself will give u the pass and he won't even know about that. So research is being done in this case to avoid such attacks.

Hackers hack servers easily by Web server intrusion method. Internet Information Services web servers are most popular among business organizations. Exploits are released and hackers take advantage of it and hack servers. Hackers can do penetration tests on servers and most of them succeed in getting into internal network. It becomes difficult to track the intruder if he is silent or does not do anything which alerts admin of cautious behavior. To know about such activity event log monitoring system is used which tells the webmaster that who logged in, in what time did he logged in and what actions were performed by him. So the webmaster gets notified by such events and he can take action immediately.

The other technique used mostly is URL Poisoning. In this method the hacker hacks a server and then inserts such ID no in the URL that whenever the user visits these sites, he is being logged, whatever page he visits on that site is being logged so this becomes difficult for the user to get rid off and his privacy is revealed. Research is being done on it to avoid such attacks.

Research is also being done in Remote File Inclusion, it allows the hacker to include scripts into the URL which are executed by the websites and the action is performed. This process can be done to deface a website or to steal information from the server. Hackers mostly upload shells (scripts) which give you full access to site and then using some techniques and software's like netcat allows you to root the server and gain full access of the server. Research is being done for avoiding remote file inclusion as well as local file inclusion.

To do away with these Trojans, DDos attacks and avoiding such attacks I will suggest some software's that should be lodged on your pc. To avoid Trojans, use antivirus "Kaspersky", you can find it on its authenticated website. And with it download any anti-malware software, but be careful before downloading and check the site if it's legit or not, because now-a-days, many fake sites are providing anti-malware software's but they have attached Trojans in those software's, so you can easily be fooled and get infected.

Two techniques you should be using while downloading anti-malware software is that, first off all check the ranking of the site on Google.com, if the site is placed on first 3 pages, then it can be legit and can be trusted, otherwise software's lying on 5 and so on mostly fake. After you explore a website, check its views and comments if posted by members or the people who downloaded it. You will become adept in whether it is legit or not. Download it and even after that you don't fully trust that software, scan it on any online scanner and you will get satisfied by the results. The other way to know if you are infected by Trojan or not is to check through command prompt. I will lead you how to take care of that business. First of all, shut all the applications that are being used by internet, e.g. browser, chatting messenger etc.

Now go to Start>All Programs>Command Prompt or just go to Start>Run and then type "cmd", this will open a black screen known as command prompt, now type "Netstat" and you will see Active Connections and Established Connections, in established connections, check the foreign IP's, sometimes web address is given instead of an IP. If you see a lot of established IP 's this might be a bit serious condition, copy the unknown IP from the screen and then search it on Google or simply put the IP in www.domaintools.com and if it is recognized IP, then it is safe otherwise you are infected with Trojans. Follow the security steps that I just defined above.

VI. CONCLUSION

It is to be concluded that certain steps and security measures are to be taken to avoid such attacks. To avoid getting infected by Trojans, don't go on those websites that don't look legit. Sites which have loads of ads on them are mostly infected so avoid going on these sites. And stop clicking on those pages and links which say like

"Congratulations! You have won money" clicking on these pages might infect you with Trojan or worms.

Install the antivirus on your computer and it should be registered and its virus definition should be up-to-date. Some antivirus themselves block those websites which contain malware or virus. Those sites which are infected by malware or worms etc are shown with a caution sign if searched on Google. Use strong passwords which should include special characters as well as numbers. Avoid using passwords like, cooler, stronger etc these passwords can be guessed by hacker and brute forcer too. And don't make passwords as your names. If you are a administrator and you want to store emails and passwords in database then encrypt them first and then store them, I prefer you to use private encrypters instead of public ones because public encrypters can be decoded easily whereas private can't be decoded easily.

Secondly, always use that alternate email that you not use often. If you use it regularly then chances are that you may get that account hacked, chances are less if you don't use that email very often. If you forgot password you can recover it easily on alternate email. Whereas in case of secret question, always use that question whose answer you will never forget. Many people now-a-days forget the answers to there security questions. If you have a good memory then change secret question after every 2 month.

To avoid Denial of Service attacks, use those web servers that are DDos free, check your system regularly for any suspicious activity going on. If you don't have DDos free server then there can't be done anything for it. DDos can be a bit disturbing but it won't affect the server it will just make it slow for the timeframe in which it is being ddos'ed. The most dreadful effect that it has is that you loose clients and customers which come on your website and see a message "Server Down".

Always keep your computer and antivirus up-to-date. Because of this flaws that have occurred in previous versions are removed in newer version and your system becomes risk free. Use those antiviruses which are registered. While browsing don't download those software's, programs, applications that you don't trust. If there are limited no of copies available on internet then download it but don't run or execute it, especially files with .exe extension. Download sandbox and run on it or use any online virus scanner to scan the file for viruses. Always activate your firewalls; mostly viruses are stopped by them. Don't give access to any person who you don't trust fully some people install key logger on your system and hide it and get all your passwords and you don't know the reason where they are being leaked. To avoid such network security attacks follow these steps and happened to be on the safe side.

VII. REFERENCES

[1] Cryptography and Network Security: Principles and Practice (5th Edition) by William Stallings

[2] Network Security by Scott C.-H. Huang, David MacCallum, and Ding-Zhu Du

[3] A Novel Quantitative Approach For Measuring Network Security Ahmed, M.S.; Al-Shaer, E.; Khan, L.; INFOCOM 2008. The 27th Conference on Computer Communications. IEEE

[4] Context-Aware Session and Network Control in Future Internet Neto, A. Sargento, S. Pinto, F.C. Logota, E. Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference

[5] Future network applications, Network Model, and development strategy Jun Dou Yu Xia Xi Chen Broadband Communications, Networks, and Systems, 2009. BROADNETS 2009. Sixth International Conference

[6] Network Security: A Decision and Game-Theoretic Approach By Tansu Alpcan, Tamer Basar

[7] Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide)by Catherine Paquet

[8] Hacking exposed 6: network security secrets & solutions By Stuart McClure, Joel Scambray, George Kurtz

[9] A Node Architecture for 1000 Future Networks Volker, L. Martin, D. El Khayaut, I. Werle, C. Zitterbart, M. Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference

[10] Security for Process Control Systems: An Overview Brundle, M.; Naedele, M.; Security & Privacy, IEEE Volume: 6 Issue:6