International Journal of Research (IJR) Vol-1, Issue-11 December 2014 **ISSN 2348-6848**

Network Security

Shashank Thakur, Shivani Chauhan, Sheetal Rana & Saurav Sharma

Department of Computer Science Engineering, Dronacharya college of Engineering, Gurgaon (Haryana) INDIA
Email: shivanichauhan2011@gmail.com

ABSTRACT:
Wireless networking is one of the most growing technologies for sensing and performing the different tasks. Such networks are beneficial in many fields, such as emergencies, health monitoring, environmental control, military, industries and these networks prone to malicious users' and cyber attacks. Network Security issues are now becoming important as society is moving to digital information age. Data security is the utmost critical component in ensuring safe transmission of information through the internet. It comprises authorization of access to information in a network, controlled by the network administrator. The task of network security not only requires ensuring the security of end systems but of the entire network. Network Security has become very important in today's world, as a result of which various methods are adopted to bypass it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. This paper outlines the various attack methods which are used, as well as various defence mechanisms against them.

Keywords: DOS attacks, Firewalls, Encryption, measures.

INTRODUCTION:

With the progress of time, computer technology has been greatly developed and today's network communication system has spread to every corner of the world, involving political, economic, military and all walks of social life. It plays an extremely important role. However, besides fun and convenience, computer also brings to us a lot of security risks due to its openness and connectivity. Users are now faced with a large number of security threats. Is computer network safe? Criminal cases are frequently visitors of domestic and international coverage. Network security refers to protecting the websites domains or servers from various forms of attack. Having the knowledge of how the attacks are executed we can better protect ourselves. The architecture of the network can be modified to prevent these attacks, many companies use firewall and various polices to protect themselves. Network security has a very vast field which was developed in stages and as of today, it is still in evolutionary stage. To understand the current research being done, one must understand its background and must have knowledge of the working of the internet, its vulnerabilities and the methods which can be used to initiate attacks on the system. Internet has become more and more widespread, in today's world internet is available everywhere in our house, in our work place, mobiles, cars everything is connected to the internet and if an unauthorized person is able to get access to this network he can not only spy on us but he can easily mess up our lives.

A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses". The synchronous network consists of switches and since they do not buffer any data and hence are not required to be protected. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. As forecasting goes for the field of the network security it can be said that some new trends are emerging some are based on old ideas such as biometric scanning while others are completely new and revolutionary. Email is a widely used service today and it is also contain many serious flaws, there is no system of authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can be easily intercepted and changed. SPAM are

serious security threat they only require very less manpower but affect millions to billions of Email users around the world, they can malicious link or even false advertisements. A network contains many vulnerabilities but most of them can fixed by following very simple procedures, such as updating software and correctly configuring network and firewall rules, using a good anti-virus software etc. In this report most of the basic information regarding network security will be outlined such as finding and closing vulnerabilities and preventing network attacks and also security measures currently being used.

CURRENT SITUATION OF COMPUTER NETWORK SECURITY

- The idea security of computer network

The computer network security we talk about actually is the security of computer network, security of important data in the network system and the structural completion of computer network. To accomplish computer network security is to protect users' data and computer system from malicious attacks and steals from outside. People who work on protection of computer network security are technical material analysis engineer of computer network security. They protect the network system from computer security problems that would influence the security of users' computers, like steal, collapse, interrupt and etc.

- Current developmental situation of computer network security

Nowadays, computers are popularized and became an indispensable part in people's life. People use computer network communication technology to communicate with friends, finish works, learn new knowledge and entertain themselves. The development of computer technology is changing people's way of living and improving the quality of life. However, computer network security still bothers people. It is a serious problem to China and the world. There are a lot of computer network security specialists working on in-depths researches in computer network security. They have set up special researches on the maintaining, destruction and repairmen of computer network security. Based on these research results, specialists built the PPDRR computer network security model. Through the PPDRR computer network security model, people can accomplish monitoring and analyzing computer network security. Through the PPDRR computer network security model, specialist can detect the vulnerabilities of computer network system and react in time to protect computer network system from leak of information and economical loss.

INFLUENTIAL ELEMENTS OF SECURITY OF COMPUTER NETWORK

ATTACK OF HACKERS:

Hacker refers to people with great computer network skills but use them to sabotage the internet or steal information. Currently, hackers are the number 1 influential element of computer network security. The main operational principle of hackers' attack on computer network security is to use their great skills of computer network to enter the system to collect data. Then they use collated data to monitor every computer in the network system to find the vulnerability of the network to sabotage the system and destroy computer network security system. Most hacked use Trojan horses and worm virus to attack users' computers. Some hackers with great knowledge base would also write large amount of false programs to install on users' computers to control their computers. Some hackers would also monitor user's internet data to steal users' account numbers, passwords and bank savings. Users would have great loss. In order to protect users' personal information and avoid malicious consequences, we need to set up a computer network security model to monitor internet security. There would be threats like communication threat, application treat and system threat in hackers' attack. Communication attack refers to the situation that users' information in communication is required by a third party. Application threat refers to that in the working process of computer network, because

of programs leaks users' information is leaked to hackers and creates loss. System threat refers to the threat where system vulnerability resulted in hacker attack.

SOFTWARE SYSTEM AND VULNERABILITY OF NETWORK SYSTEM:

In computer network security, vulnerability of network and software is the second influential element of computer network security after hacker attack. Vulnerability of computer network and software includes vulnerability in computer system and software design, lack of protection of computer network and software security, illegal users enter users' computer through computer network vulnerability and computer being controlled maliciously by unknown users. This high-risk vulnerability could severely influence user's daily use of computer and normal network communication. It would cause users' information cannot spread and receive. With this high-risk vulnerability, computers could be attacked; information could be stealed any time by any unknown people. It would directly influence the security of computer network system and cause great loss.

FALSIFICATION OF USERS' PERSONAL INFORMATION AND LEAK OF CLASSIFIED INFORMATION:

Falsification of users' personal information and leak of classified information is the third element of computer security. In the whole process of computer network communication, information got spread the most is personal information of users and classified materials. Therefore, we must pay special attention to the protection of users' personal information and classified materials. Falsification of users' personal information refers to the action that with the transfer of users' information, a third party intercept, falsify and delete the information to result in the interception and steal of users' information. Leak of users' information refers to unknown personnel monitor users' computers remotely and steal information through computer network. Illegal transfer of users' information refers to the illegal steal or borrowing of information without the acknowledgment and permission of user meanwhile create loss. Nowadays' society is a society of technology development. The universal use of computer technology has a great influence on people's life. Computer network technology has influences on people's life, economy and politics. But this kind of influences is two-sided. There are good influences and bad influences. Computer network technology brings people's life convenience and threat to the security of personal information. This vulnerability of computer network security brings lot problems and causes the users of computer network great loss.

DIFFERENT TYPES OF SECURITY ATTACKS

- **Passive Attacks**

This type of attacks includes attempts to break the system using observed data. One of its example is plain text attack, where both the plain text and cipher text are already known to the attacker.

Properties of passive attacks are as follows:

• Interception: The data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks

• Traffic analysis: Also attacks confidentiality. It can include trace back on a network like a CRT radiation.

- **Active Attacks**

In this attack the attacker sends data stream to one or both the parties involved or he can also completely cut off the data stream.

Its attributes are as follows:

• Interruption: It prevents an authenticated user form accessing the site. It attacks availability. Such as DOS attacks.

• Modification: In this the data is modified mostly during transmission. It attacks integrity.

• Fabrication: Creating counterfeit items on a network without proper authorization. It attacks authentication.

- **DOS Attack**

DOS attacks today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don't require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affects availability of the network. With the help of easy to use network tools such as Trinoo, which can be easily downloaded of the internet any normal user can initiate an attack. DOS attacks usually works by exhausting the targeted network of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DOS attacks use many users connected to a network known as zombies most of the time users are unaware of that their computer is infected.

Different Types of DOS Attacks

Many attacks are used to perform a DOS attack so as to disable service. Some of which are as follows: TCP SYN Flooding. When a client wants to connect to the server, the client first sends to an SYN message to the server. The server then responds to the client by sending a SYN-ACK message to the client. The client completes the connection by sending an ACK message. The connection is now established and data can be transferred easily. The problem arises when the connections remain half open and the server waits for the client side to send an ACK message. This takes system resources and the server will wait till the expiration date. The person exploiting the server will never send the ACK message and will keep on sending new connection demand, till the server is overloaded, thus cannot provide access .

ICMP Smurf Flooding: ICMP package is used to know whether the server is responding or not. The server replies with an ICMP echo command. In smurf attack the attacking host forges the ICMP echo requests having victims address as the source and the broadcast address of remote networks. These computers will then send back ICMP echo reply package to source, thus congesting victim's network.

MEASURES TO IMPROVE NETWORK SECURITY

ONLINE ANTI-VIRUS MEASURES.

According to the characteristics of computer network virus, effective prevention on the virus is difficult and complex. It is a daunting task for network managers to monitor the prevention work. Previous work is only limited to every client computer, in which every user needs to install anti-virus software and on your machine, such as KV300 system, or Rising anti-virus software, etc. However, due to limited computer skill of users, this approach is hard to ensure the safety of the whole network system. As an effective solution to prevent the, the basic requirement is to meet the following demands:

1. Install anti-virus software on computers
1. Update the virus database in users' machines
2. Released the latest virus database upgrade file from the WAN connection
3. Coordination and management of remote users' virus scanning
4. Address user-reported problems timely
5. Download and preview scan report provided by users
6. Remote control user options
7. Improve the execution speed and zooming ability in large-scale networks

People are more capable of preventing online viruses. More anti-virus measures have emerged in order to effectively guarantee the network security. Network management personnel can install a complete set of virus software on any client server through one source server. As there are many types of software, network managers should take into account their own situation to achieve the "best use." When choosing solutions, managers should address current situation and leave room for further developments.

MEASURE TO PREVENT HACKERS.

The invasion and attack can be divided into subjective and objective security issues. Subjectivity security issue mainly refers to errors made by network management personnel. Objectivity security issue mainly refers to loopholes in computers and the network where hackers exploit these vulnerabilities to conduct various forms of attack.

USE SAFETY TOOL

The above-mentioned basic techniques of computer network security can collect safety issues of host computers. Network management personnel identify these problems in a timely manner and install the patch. Network managers take the advantage of scanning tools (such as NAL's Cyber Cop Scanner) to scan host computers, learn about the weakness links take appropriate preventive and repair measures.

FIREWALL TECHNOLOGY

It is the most widely sold and available network security tool available in the market. This is the wall which stands between the local network and the internet and filters the traffic ad prevents most of the network attacks. There are three different types of firewalls depending on filtering at the IP level, Packet level or at the TCP or application level . Firewalls help preventing unauthorised network traffic through an unsecured network to a private network. They can notify the user when an untreated

Application is requested access to the internet. They also create a log of all the connections made to the system. These logs can be very harmful in case of any hacking attempts. Firewalls only work if they are correctly configured, if somebody makes a mistake while configuring the firewall, it may allow unauthorised to enter or leave the system. It takes certain knowledge and experience to correctly configure a firewall. If the firewall goes down one cannot connect to the network as in a case of DOS

Attack. Firewall also reduces the speed of network performance as it examines both incoming and outgoing traffic. Firewall does not manage any internal traffic where most of the attacks come from. Many companies are under false assumptions, that by just using a firewall they are safe, but the truth is they are not, firewall can be easily be circumvented. The best thing while configuring firewall is to deny anything that is not allowed In short, firewall technology is to prevent others from accessing your network device like a shield. There are three types of firewall technology, namely, packet filtering technology, agent technology, and status monitoring technology. Packet filtering technology is to verify the IP address by setting it. Those IP addresses that do not match those settings will be filtered by the firewall. But this is the first layer of protection. Agent technology is to verify the legitimacy of requests sent by accept client of proxy server to. This technology also involves with user authentication, login, simplified filtering criteria and shielding the internal IP addresses. Status monitoring technology is the third generation of network security technologies, which is effective for all levels of network monitoring. It makes it possible to make timely security decisions. Firewall technology can successfully prevent hacker from intrusion in the local network and protect the network.

DEFENCE AGAINST DOS ATTACKS

To prevent DDoS attack many technologies have been developed such as intrusion detection systems (IDSs), firewalls, and enhanced routers. These things are used between the internet and servers. They monitor incoming connections as well as outgoing connections and automatically take steps to protect the network. They have traffic analysis, access control, redundancy built into them .IDSs are make a log of both the incoming and outgoing connections. These logs can then be compared to baseline traffic to detect potential Dos attacks. If there is unusually high traffic on the server it can also alert of a possible ongoing DOS attack such as TCP SYN flooding .Firewalls can also be used as defence against DOS attacks with the required configuration. Firewalls can be used to allow or deny certain packets, ports and IP addresses etc. Firewalls can also perform real time evaluation of the traffic

and take the necessary steps to prevent the attack. Security measures can also be employed in routers which can create another defence line away from the target, so even if a DOS attack takes place it won't affect the internal network. Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible. If the service providers are able to distribute the heavy traffic of a DOS attack over a wide network quickly it can also prevent DOS attacks, however this method require computer and network resources and they can be very costly to provide on daily basis as a result only very big companies opt for this method.

MEASURES ABOUT SWITCH

When designing a large-scale regional computer network, we need to ensure that the switch is connected to a network or in a separate network, so that the switch can form a separate management network. This will effectively reduce the number of network switches and narrow the scope of failure. By using search and location, it is also convenient for network managers to quickly handle remote network accidents.

ENCRYPTION

Using encryption methods one can prevent hacker listening onto the data because without the right key it will just be garbage to him .Different encryption method such as using HTTPS or SHTTP during the transmission of data between the client and user, will prevent Man in the middle attack (MIM), this will also prevent any sniffing of data and thus any eavesdropping. Using VPN will encrypt all the data going through the network; it will also improve the privacy of the user. Encryption also has downsides as all the encrypted mail and web pages are allowed through firewall they can also contain malware in them. Encrypting data takes processing power from the CPU. This in turn reduces the speed at which data can be send, the stronger the encryption the more time it takes.

E-MAIL SECURITY

As both the sender and receiver of the email one must be concerned about the sensitivity of the information in the mail, it being viewed by unauthorised users, being modified in the middle or in the storage. Email can be easily counterfeit therefore one must always authenticate its source. E-mail can also be used as a delivery mechanism for viruses. Cryptography as in many other fields' plays a crucial role in email security .Emails is very unsecure. As they pass through many mail servers during transits they can be easily intercepted and modified. While using common Email there is no process to authenticate the sender and many users would not give a thought to authenticate the email received. There are many standards one can choose in order to secure his emails some of these are: PGP, PEM, Secure multipurpose Internet mail extension (MIME), Message Security Protocol (MSP). The emails during their transit are stored in many servers, which they pass through during their transit and as a result they are not actually deleted when the users delete them from their account. These copies can be easily retrieved and as well as their contents. Thus there should be a feature to delete these copies or making these copies secure basically by using some strong encryption so that they cannot be read.

ADVANCES IN NETWORK SECURITY

Before the internet became popular and fairly common, intrusion detection meant detection of an unauthorized human user/person on a machine, but this definition radically changed with the advent of Code Red worm and its variants in the year 2001. These were 1st generation worm they had high spread rats and made human countermeasures impossible. A real-time and an automated system were to be developed to detect and prevent further spread of these worms. These worms generated high traffic especially on Port 80, therefore a volumetric approach was proposed to detect them. It worked for the generation where network infrastructure was not widely deployed. However they became useless in the recent years because of the

behaviour of worm is now specific in many cases and also users begin to generate high volume on their own using file sharing sites and network gaming. Network security is being improved in two fields namely hardware and security in the following ways:

HARDWARE DEVELOPMENT

This field is not developing very rapidly as its software counterpart but nonetheless some amazing developments are being made such as using Biometric systems and smartcards which can drastically reduce the number of unauthorised access. Biometric has very important use in the field of the network security, some obvious uses such a built in biometric scanner attached to a workstation can be used as an authentication mechanism which can be used as a login to the system, since two persons cannot have the same biometrics as the both persons, it is a full proof mechanism of login .People tend to forget their passwords and so they keep it near their workstation written on a slip or something else or even lock themselves out of their system by incorrectly entering it too many times. All this can be easily avoided by biometric systems as they provide users undeniable proof of identity. Smartcards are provided by companies to its workers, they only work when they are inserted in the computer and a pin issued the network administrator is entered, since the pin issued is only four characters and numeric, users don't forget it and don't write it down.

SOFTWARE DEVELOPMENTS

The software field is very wide when it comes to network security. It includes firewall, antivirus, VPN, intrusion detection, and many much more. The improvement of network security is basically still the same. When new virus are found virus definitions are updated, it's the same for firewalls instead their rules are updated. As more and more security transits to hardware such as biometric. The software must be able to use the information correctly and appropriately. Currently research is being focused on neural networks for facial recognition software. Most current algorithms require substantial processing power. This power cannot be available in small devices like sensors. Therefore, one must develop light weight algorithms to counter this problem.

Antivirus works on a very basic principle; they scan a file and then match its digital signature against the known malwares. If the signature is match in the database it reports it, delete it or even disinfect it depending on the user's setting. This system however easy has a huge drawback, whenever a new malware is found; it takes time before the antivirus database can be updated and during this period the malware can already take complete control of the computer, disables the antivirus or even hides itself from the antivirus. To prevent this antivirus companies introduced a new system called cloud scanning this way not only wills the digital signature be scanned across the database but also across millions of computers and servers across the world. This all happens and real time and results are very fast. This greatly reduces the chance of infection from a new malware.

CONCLUSION

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defence secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Even a small unnoticed vulnerability in a network can have disastrous affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Computer network security is a complicated issue, involving many aspects of computer technology, network management, network usage and maintenance. In order to increase computer network security, we should mix various types of applications for protection measures. It is necessary to develop more effective security solving measures, thereby to improve the

computer network security prevention and. It is a long way to go to ensure the normal operation of large-scale network system and communication and maintain sustainable and efficient transport network. To build a harmonious secure computer network security system, we need to take advantage of a variety of integrated network security and green data networking products to form an intelligent network protection system, and thus make computer network security meet various needs. All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor also.

REFERENCES

[1] B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[2] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.

[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[4] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University,2010.

[5] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

[6] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.

[7] [Online]Available: http://www.duosecurity.com.

[8] [Online]Available:http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%20Technique.pdf.