Network Security

Anuj kumar Bishnoi & Priyanka Khatri
(Student, Department of Information technology
Dronacharya College of Engg. Gurgaon, Haryana
(anuj199229@yahoo.com); (msg2khatri@gmail.com)

ABSTRACT

One of the most important parts to personal computer users is network security. Security has become a topic of importance by the expansion of internet. The architecture of the internet when modified can shrink the possible attacks that can be sent across the network. The research paper is an overview about the various incidents that have occurred in internet's lifetime. It has discussed about the various technologies that have been developed so far to prevent the network security. Apart from this it has also thrown light over the secure methods which an organization or an individual can take on for the security of their essential data. Whenever we research about something we must know about how it evolved, so we have discussed over that issue also. Knowing the attack methods, allows for the right security to emerge. Many businesses shelter themselves by the means of firewalls and encryption mechanisms. The businesses form an INTRANET to remain linked to the internet but secured from possible threats.The entire field of network security is immense and in an evolutionary stage. The range of study encompasses a brief history dating back to internet early stages and the existing technologies used to overcome network security. In order to understand the research being performed today, knowledge of the internet, attack methods through the internet, and security knowledge is important and therefore they reviewed.

KEYWORDS:-

E-commerce; password; cryptography; internet protocol; encryption

INTRODUCTION

The world is becoming more interconnected with the arrival of the new internet networking technology.There ishuge amount of private, commercial, military, and government information on network infrastructures wide-reaching. Network security is becoming of great significance because of intellectual property that can be acquired on internet.

Fundamentally two different and synchronous networks are available on internet. The internet is considered a data network. Since the current data networkconsists of computer-based routers, information can be obtained by unique programs. The synchronous networkwhich instead of buffer data consist of switches and therefore are not threatened by attackers. This is the reason behind security is emphasized in data networks, such as the internet, and its links [1].

1.1 HISTORY (TRADITIONAL VIEW)

Elucidatingour history once again when Arpanet was revealed, very little of it was designed or implemented with declaration and security as the main concern. On those times attackers or the hackers were not that intelligent that they could disrupt the system. Internet protocols were not developed to secure themselves. Within the TCP/IP communication heap, security protocols are not implemented. This leaved internet unlock to attacks. The Arpanet took birth on1969 which initiated internet.

In 1980's an ordinary language for internet computers was found known asTCP/IP protocol. For the first time a free collection of networksprepared up the ARPANET nowviewed as internet. The internet was used by the corporations to be in touch with each other and with their customers.

In 1990s the internet became widespread and continued with the development ofmore browser for which NETSCAPE and MICROSOFT are in tough competition. Ever since then internet is rising on high peak and internet surfing has become equivalent to viewing TV for many users. Information securityunderway before the internet developed.For information security cryptographer's developedanpuzzled machine to convert plain messages to encrypted text. An intelligent mathematician broke the codein 1930 which was later named as word "hacker" by some students in 1960's. Earlierinternet was limited to government contractors and academic researchersbut it was Telnet protocol which made internet public.

The hacking and crimes regarding computers started to begin at that time. In 1986 an act was created because of LAN MURPHY'S crime of thieving information from military computersfor computer fraud and abuse. A graduated student spread MORRIS WORMover 6000 susceptible computer connected to internet. Due to this CERT(computer emergency response team) was formed to aware computer users.

Subsequently security became a great concern as over 1000s of people surfed on internet at the same point of time. The security breaches can consequence into monitory losses to a greatamount. Investment in good security should be the primary priority for large organizations as well as for general users.

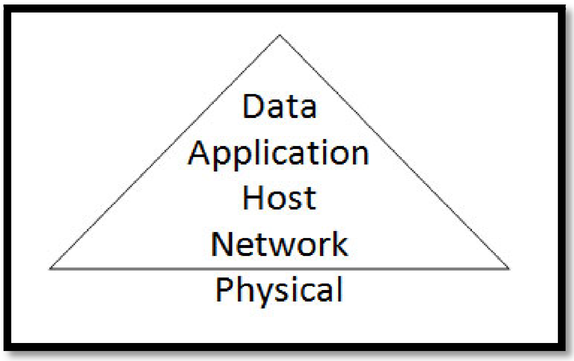

Figure1. Historical approaches to security

1.2 WORST MOMENTS OCCURRED IN NETWORK SECURITY

As time does not remain the same, so not all days are just as good as than others when we come across the term network security.Here are some our picks for some of the pits in history [3].

1.2.1 Yahoo, Dell,, eBay,Amazon and CNN all once struck down by a massivespreading of denial-of-service attack because of a teen calling himself "MAFIABOY". He has beentrapped and sentenced to eight months of "open custody," anything that means, a light fine and limited use of the Internet.

1.2.2 The "ILoveYou" worm scoots from Hong Kong around the world in seconds, affecting an expected 10% of all connected computers. It over flooded Inboxes of several organizations, counting the Pentagon and British Parliament which brought Business serversonto their knees.

1.2.3 A neighbouring country to Russia named Estonia, of about 3 million people, had a powerful network infrastructure that came under a severe cyber attack that made its central government, banking and media Web sites unavailable. Security experts examined the cyber attack supposed that it was head out by the "Russian blogosphere," which triggered a second phase that incorporated specially designed bots, dropped onto home computers.

1.2.4 Arpanet annoyed but presently we are with one and only internet.Digital Equipment Corp. marketing guy GARY THUERK got technical support to send what's measured as the first "spam" message to thousands on the government-funded Arpanet, predecessor of today's Internet. Arpanet management named the mass e-mail as a "flagrant violation" of Arpanet policy. Brilliant thing was they pinched that in the bud.

1.3 TYPES OF THREATS

1.3.1 PASSWORD CRACKING

It involves special types of vulnerabilities and decrypting techniques. Brute force attempt is the most popular form of cracking password. Brute force attack is a way of cracking an individual's username and password for a particular website by scanning thousands of familiar terms, words and names until a mixture of them is given to the server.

1.3.2 DENIAL OF SERVICE ATTACKS

These generallyoverwork a server andturn them intoworthless. The server is frequently asked to perform tasks that have need ofusing a large amount of resources until it can no longer function correctly.

1.3.3 SERVER USER EXPLOITS

It allows attackers to gain power of a system as if they were an administrator. They time and again use scripts to manipulate a database or a buffer overflow attack that cripples a system.

1.3.4 TORJANS

The software is considered to be the most unsafe in terms of E-Commerce security due to its capacity to connect behind closed doors and send confidential information. These are the special programs developed for specific purposes of communicating without the option of detection.

1.3.5 IP SPOOFING ATTACKS

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to getway in to other computers. The identificationof the intruder is invisible by different means making detection and prevention complex.

1.4 TECHNOLOGIES DEVELOPED FOR NETWORK SECURITY

It is obvious that when something is made free its security decreases. Since internet contains and communicates with data so threats will always remain a foremost concern. To avoid useless access, defence and detection mechanisms were developed.

Web developers and security professionals must apply and make use of effective security techniques and policies. Technology management must pursue the three R’s of security – recognize, resist, and recover [4].

1.4.1 CRYPTOGRAPHIC SYSTEMS

It prevents the data from being misused via converting the data into codes and ciphers into an insignificant data. Encryption and decryption occurs at receiver and server end only.

1.4.2 FIREWALL

The purpose of firewall is to sort out communications that may be ominous to a system. It restricts traffic to a system and allows pre-determined activity to go through filter. It is a usual border control mechanism or perimeter protection. The intention of a firewall is to obstruct traffic externally, but it could also be used to block traffic within. A firewall is the forefrontdefence mechanismin opposition to intruders. It is a system designed to avoid unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a permutation of both [5].

1.4.3 INRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is asupplementary protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to identify an attack. IDS products are used to supervise connection in determining whether attacks are been launched. Some IDS systems just monitor and vigilant of an attack, whether others try to obstruct the attack.

1.4.4 ANTI-MALWARE SOFTWARE AND SCANNERS

VIRUSES, WORMS and TORJAN horses are all examples of spiteful software, or Malware for short. Special so-called anti-Malware is used to identify them and cure an infected system.

1.4.5 SECURE SOCKET LAYER(SSL)

The secure socket layer(SSL) is a suite of protocols that is a standard approach to achieve a better level of security between a web browser and a website. It can be said that it is a type of encryption between a client and a host.All communications when stopover a page with confidential information are encrypted before they are sent over internet.

SSL is designed to build a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected inside the protected tunnel. SSL provides verification of clients to server through the use of certificates. Clients present a certificate to the server to confirm their identity. Through this even if a hacker is capable to intercept data packets from the information being exchanged, the hacker would require the tools that could decrypt the files.

1.4.6 SECURITY ISSUES OF IP PROTOCOL

The IPV6 is a substantial advancement over the IPV4 internet protocol. Regardless of the IPV6’s great security mechanisms as from a security viewpoint, till now it continues to a vulnerable to threats. Here are listed some areas of the IPV6 protocol still create a potential security issue.

Latest internet protocol is not guard againstthe misconfiguredtypes of servers, with feebly designed applications, or poorly protected sites.

The probable security problems come out due to the following:

1. The Header manipulation issues.
2. The Flooding issues
3. TheMobility issues

The Header manipulation issues basically occur due to the known IPsec's implanted functionality. The Extension headers detect some of the general sources of attack of header manipulation. The difficulty is that the extensions headers need to be get processed by all stacks, and canguideup to a long chain of extension headers. Large numbers of extension headersovercome a type certain node and it is a type of attack if it is purposeful.Spoofing continues it to be security danger on IPv6 protocol.

There is also a type of attack called as port scanning occurs when there is anentire section of a network which is scanned to get potential targets with open services. There is an address space of the IPv6 protocol which is outsizedbut the protocol therefore is still not safe to this type of attack.

A new feature,Mobility, is that which is included into the internet protocol IPv6. This feature requires the unique security measures. Network administrators also need to be in awake of these security needs while using IPv6's mobility feature.

1.4.7 EFFECTIVE PASSWORD POLICIES

Implementation of the password policies which are helped to weaken out a password cracker's whose usefulness is essential. Accounts intercepts should be locked out after a scheduled number of consecutive erroneous username and password combinations. The ensurance is that users utilizing the brute force attack are not being able to repeatedly attempt the login combinations. The IP address of thoseare blacklisted on the web server. As Minimum password lengths and the maximum occurrences of exact character may be two of many ways to enhance security.

1.4.8 ONE-WAY HASHING ALGORITHMS

To Secure the one way hash functions we have to use a fingerprint on the basic of each data packet so that both are of a web server and client so can confirmthe data reliability. The One-way hash functions hand out many purposes, such as encryption, integrity checking, and authentication.MD5 algorithm is one which the System administrators often use toconvey large files data or while downloading the updates for systems in order tomake sureof the integrity of the data so that they may do not install the software that may have unsafe code or TORJANS.

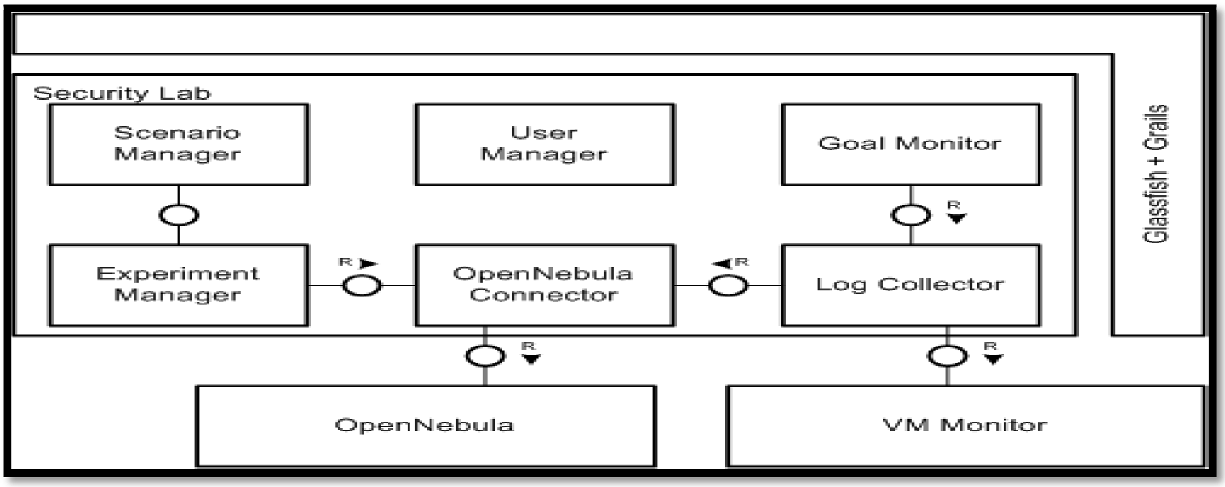

Figure2. Virtual security experimental framework

1.5 STEPS TOWARDS A SAFE NETWORK

Security must not be treated as an annoyance. It is more than just averting or restraining what people do. A good security enables the industries to operate their works safely and securely by shielding revenue and profits that could be lost through data. The most essential part of your bull is treat security. Then comes a time when we can move towards a safe system where there is full security. Generally the nasty cyber associated with conducting and dealing from weeks for buildings and broad and effective contracts. There is a look for agenda that builds an expectation and means for dealing for changing skill and ethics of a detailed problem which is basically unbounded time into future as well as building the abilities of weaker countries.

1.5.1 The effort regarding the serious offenses which are against computer networks. The most complicated and crucial concern is to protect the organization which is either an IT based organization or an organization that may be retrieved and damaged or manipulated through IT-based control structures.

1.5.2 There must be an organization of laws which should agreement with state party and adopt a complete diagnose of national laws which either will punish the serious crimes against the computer diagnose of national laws which either will punish the serious crimes against the computer security network. The working of these laws is different in different countries as a result of malicious behaviour specify as offences within the country. Such enacted would be an admission to the agreement as the necessary condition.

1.5.3 The state receives are the set of near universal which is basically a global problem. The near universal participation makes a problem globally. Each and every country which is either connected to the internet or is a global network is a part of hazard and the exposure problem there must be an effort which will try to make a solution to this.

1.5.4 A major goal to deal with the problem is to build international aptitude. We must develop or go through the organization which would help us to develop the standards based applies and provide training and the technologies. On a global ruler and to domicile those countries which have no plies, and provide training and technology on a global ruler, and especially for the large number of countries that have little or no capacity to do everything for them in the replicated domain this time. This applies to both energetic and inactive means of defence.

1.5.5 Avoid building too much technical or practical detail into the basic contract. At this time, no one understands the industrial and procedural means or costs well enough to appreciate what it would take to require them on a large scale. It is suggested to setting up a forum and means, for the necessary deliberations and work to take place.

1.6 CONCLUSIONS

Network security is ansignificant field that is ever more gaining interest as the internet expands. The security threats and internet protocol were examined to resolve the required security technology. The security technology is mostly software based, but many frequent hardware devices are used. The present development in network security is not very notable. Initially it was understood that with the significance of the network security field, new approaches to security, both hardware and software, would be intensely researched. It was shocking to see most of the development taking place in the same technologies being currently worn. Collective use of IPV6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will confirm

Efficient in guarding intellectual property for the near future. The network security field may have to develop more rapidly to deal with the threats further in the future.

1.7 FUTURE TRENDS IN SECURITY

What is going to determine the internet security is the set of claims more than anything else. The future will possibly be that the security is similar to a safe system. The safe system fights off attacks and builds itself to fight harder enemies. Similarly, the web security will be able to work as an immune system.

The drift towards biometrics could have taken place a while ago, but it seems that it isn't being actively chased. Many security expansions that are taking place are within the same set of retreat technology that is being used today with some more modifications

1.8 REFRENCES

[1]Stallings, William. *Network and Internetwork Security: Principles and Practice*. Englewood Cliffs, NJ: Prentice Hall, 1995.

[2]Amoroso, Edward. *Fundamentals of Computer Security Technology*. Englewood Cliffs, NJ: Prentice-Hall, 1994.

[3]Brunner, John. *Shockwave Rider.* New York, NY: A Del Ray Book, published by Ballantine, 1975.

[4]Carroll, John M. *Computer Security*. 2nd edition, Stoneham, MA: Butterworth Publishers, 1987.

[5]Bellovin, Steve and Cheswick, Bill. *Firewalls and Internet Security*. Reading, MA: Addison-Wesley, 1994.

[6]Liu, Cricket, Jerry Peek, Russ Jones, Bryan Buus, and Adrian Nye. *Managing Internet Information Services,* Sebastopol, CA: O'Reilly & Associates, 1994.