ISSN 2319 – 7757 EISSN 2319 – 7765

Indian Journal of Engineering

Network security is a key for internet users: a perspective

Pooja Agarwal[1], Pooja Yadav[2], Neelam Sharma[3], Ruchika Uniyal[4], Swati Sharma[5]

1. Department of Computer Science & Engg. Dronacharya College of Engg. Gurgaon, Haryana, India, E-mail: ag.pooja92@yahoo.in
2. Department of Computer Science & Engg. Dronacharya College of Engg. Gurgaon, Haryana, India, E-mail: poojayadav0592@yahoo.in
3. Department of Computer Science & Engg. Dronacharya College of Engg. Gurgaon, Haryana, India, E-mail: neelam22101991@gmail.com
4. Department of Computer Science & Engg. Dronacharya College of Engg. Gurgaon, Haryana, India, E-mail: ruchikauniyal.ru@gmail.com
5. Department of Computer Science & Engg. Dronacharya College of Engg. Gurgaon, Haryana, India, E-mail: swativats07@gmail.com

Received 24 September; accepted 17 October; published online 01 November; printed 16 November 2012

ABSTRACT

Network security has become the most significant part to personal computer users and other purposes. With the discover of the internet, security has become a major intense issue. Internet structure itself permitted for countless security terrorization to occur. 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.

1. INTRODUCTION

The world is becoming more interconnected with the arrival of the new internet networking technology. There is huge 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 network consists of computer-based routers, information can be obtained by unique programs. The synchronous network which instead of buffer data consist of switches, therefore they 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)

If we enlighten our history once again when Arpanet was discovered, very little of it was designed or implemented with assertion and security as the key concern [2]. Even at that time attackers or the hackers were not so intelligent that they could disrupt the whole system. These were discovered irrespective of storing the data and were instead used for huge computations which can't be performed by human beings on hands. 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 on 1969 which initiated internet. In 1980's TCP/IP protocol was discovered as ordinary language for internet computers. For the first time a free collection of networks made up the ARPANET now visualized as internet. Corporations started using the internet to communicate with each other and with their customers (Fig.1).

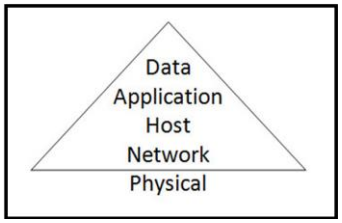

Figure 1
Historical approaches to security

In 1990s the internet became open to all. Further browser was developed for which NETSCAPE and MICROSOFT competed. Since then internet is on the rise and surfing internet has become comparable to TV viewing for many users. Information security started before the internet developed. Cryptographers developed an enigma machine to transform plain messages to encrypted text. After which in 1930 a brilliant mathematician broke the code. In 1960 some students termed a word "hacker" for this brilliancy. Telnet protocol made internet public which previously was restricted to government contractors and academic researchers.

The hackers and crimes concerning computers were beginning to come out. The computer fraud and abuse act of 1986 was created because of LAN MURPHY'S crime of stealing information from military computers. A graduated student spread MORRIS WORM over 6000 vulnerable computer linked to internet. Due to this CERT (computer emergency response team) was shaped to alert computer users. Then afterwards security became a topic of worry as over 1000s of people surfed on internet at the same time. The security breaches can result into monetory losses to a great extent. Investment in good security should be the foremost priority for large organizations as well as general users [2].

1.2. Worst moments occurred in network security

Some days are just not as good as than others when it comes to network security. Here are our picks for some of the pits in history [3].

Pooja agarwal et al.
Network security is a key for internet users: a perspective,
Indian Journal of Engineering, 2012, 1(1), 92-95,

1. Amazon, eBay, Yahoo, Dell and CNN all once struck down by a colossal distributed denial-of-service attack because of a teen calling himself “MAFIABOY”. He has been caught and sentenced to eight months of "open custody," whatever that means, a light fine and restricted use of the Internet.
2. The I Love You worm scoots from Hong Kong around the globe in seconds, infecting an expected 10% of all connected computers. Inboxes overflowed at several organizations, including the Pentagon and British Parliament which brought Business servers onto their knees.
3. Estonia, a country of about 3 million people neighboring Russia, had a intense network infrastructure that came under a serious cyber attack that made its central government, banking and media Web sites unavailable. Security experts examined the cyber attack assumed that it was set off by the "Russian blogosphere," which triggered a second phase that included specially designed bots, dropped onto home computers.
4. Arpanet irritated but here we are today with one and only internet. Digital Equipment Corp. marketing guy GARY THUERK got technical support to send what's considered as the first "spam" message to thousands on the government-funded Arpanet, forerunner of today's Internet. Arpanet management criticized the mass e-mail as a "flagrant violation" of Arpanet rules. Excellent 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 generally overwork a server and turn them into worthless. The server is frequently asked to perform tasks that have need of using 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 get way in to other computers. The identification of 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 it’s security decreases. Since internet contains and communicates with data so threats will always remain a foremost concern. To avoid useless access, defense 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 forefront defence mechanism in 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 a supplementary 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 are used to identify them and cure an infected system.

1.5. 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 is 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.

1.5.1. Security issues of IP protocol

From a security viewpoint, IPV6 is a substantial advancement over the IPV4 internet protocol. Regardless of the IPV6’s great security mechanisms, it still continues to be vulnerable to threats. Some areas of the IPV6 protocol still create a potential security issue. The latest internet protocol does not guard against misconfigured servers, feebly designed applications, or poorly protected sites (Fig.2). The probable security problems come out due to the following:

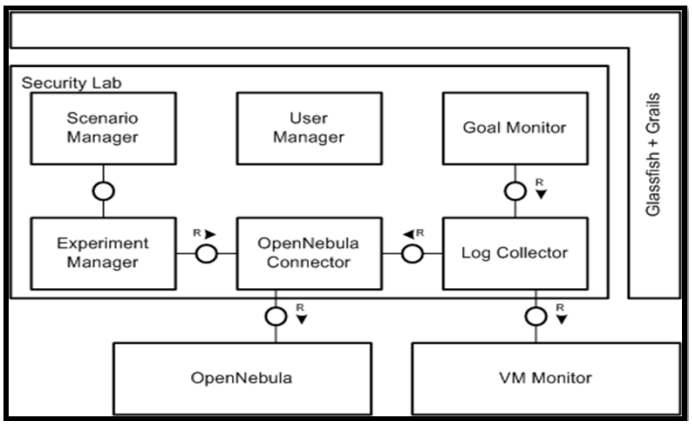

Figure 2
Virtual security experimental frameworks

Pooja agarwal et al.
Network security is a key for internet users: a perspective,
Indian Journal of Engineering, 2012, 1(1), 92-95,

1. Header manipulation issues.
2. Flooding issues
3. Mobility issues

Header manipulation issues occur due to the IPsec's implanted functionality. Extension headers deter some general sources of attack because of header manipulation. The difficulty is that extension headers need to be processed by all stacks, and this can guide to a long chain of extension headers. The large numbers of extension headers can overcome a certain node and is a type of attack if it is purposeful. Spoofing continues to be security danger on IPv6 protocol. A type of attack called port scanning occurs when an entire section of a network is scanned to get potential targets with open services. The address space of the IPv6 protocol is outsized but the protocol is still not safe to this type of attack. Mobility is a new feature that is included into the internet protocol IPv6. The feature requires unique security measures. Network administrators need to be awake of these security needs when using IPv6's mobility feature.

1.5.2. Effective password policies

The implementation of password policies that help to weaken a password cracker's usefulness is essential. Accounts should be locked out after a certain number of consecutive erroneous username and password combinations. This ensures that users utilizing a brute force attack will not be able to repeatedly attempt login combinations. Their IP addresses are blacklisted on the web server. Minimum password lengths and maximum occurrences of a exact character are two of many ways to enhance security.

1.5.3. One-way hashing algorithms

Secure one way hash functions use a fingerprint on each data packet so both a web server and client can confirm data reliability. One-way hash functions hand out many purposes, such as encryption, integrity checking, and authentication. System administrators often use a MD5 algorithm to convey large files or when downloading updates for systems to make sure of the integrity of the data so that they do not install software that may have TORJANS or other unsafe code.

1.6. Steps towards a safe network

Do not treat security as annoyance. Security is more than just averting or restraining what people can do. A good security enables industries to operate more securely by shielding revenue and profits that could be lost through data. Treat security as an essential part of your bull. Now there's a time to think about so we can move towards a safe interacting. Generally the spans associated with conducting and dealing with nasty cyber activities varies from weeks for building a broad and effective contracts. We might look to an agenda that builds in an expectation and means for dealing with the detailed problems of changing skill and ethics (Fig.3), over a basically unbounded time into the future, as well as one proposed to help build the abilities of weaker countries [6].

i. The effort should be the serious offenses against computer networks. The crucial concern is protecting the organization, both the IT based organization itself and other organizations that may be retrieved and damaged or manipulated through IT-based control structures.

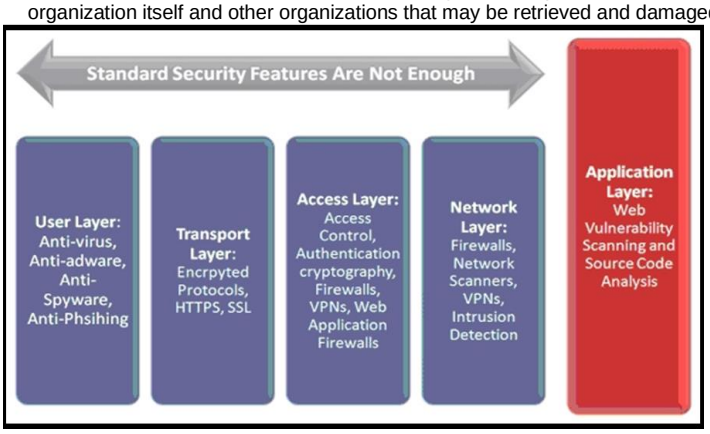

Figure 3
Required features of a safe network

ii. There should be a organization of laws. Each state party to the agreement should adopt a complete set of national laws defining and punishing the full range of serious crimes against computer networks. Although the wording of these laws need not be alike for each country, each must begin all of a collectively defined malicious behavior specified in the agreement as offenses within the country. Having such a set of enacted would be a necessary condition for admission to the agreement.

iii. There should be a near-universal set of state revelries. The problem is basically global, and at least some component of a partial solution has to be global. Near-universal participation makes the problem globally, and tries to abolish safe havens. Each country connected to the internet or other global network is part of the hazard and exposures problem, and an effort must be made to try to make each part of the solution.

iv. A major goal should be to build international aptitudes to deal with the problem. We would develop such an organization which would help to develop standards, best applies, 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 themselves in the replicated domain this time. This applies to both energetic and inactive means of defence.

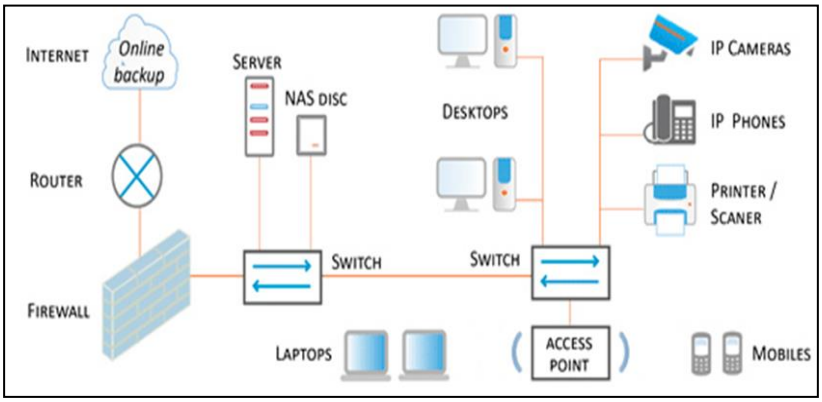

Figure 4
Basic network set up

v. 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 (Fig.4).

2. CONCLUSION

Network security is a significant 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.

3. 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 an safe system. The safe system figths 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

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.

.

Pooja agarwal et al.
Network security is a key for internet users: a perspective,
Indian Journal of Engineering, 2012, 1(1), 92-95,