Imperial Journal of Interdisciplinary Research (IJIR)
Peer Reviewed – International Journal
Vol-4, Issue-1, 2018 (IJIR)
ISSN: 2454-1362, http://www.onlinejournal.in

A Review of Network Security based on a Case Study of Medical Companies in Libya

Laila Alhimale[1], Ahmad Dabaa[2], Dineshen Chuckravanen[3]
[1]Al Jabal Al Gharbi University
[2]Al Jabal Al Gharbi University , [3]Aberystwyth University

Abstract: *Recently network security is confronting with modern threats and most of the time the defense incorporated in the system fails to prevent the damage. Financial Organisations, Governments and Army are at huge risk when attacks succeed in stealing information. However, besides this much research has been conducted in this field, and experts now possess some techniques how to manage attacks. In this paper, we speak of different attack methods that harm the security of the internet, we specify basic defending mechanisms and we also will provide up-to-date threats and modern blocking methods which are in the experimental phase. We also refer to ten companies who filled a network security questionnaire to see how robust their information technology structure is. The Future holds the insecurity of the network and also it holds upcoming defending methods. Experts already know that more effort need to be done, the war against hackers is entering a new stage with experts playing a vital role in this future fight. The internet consistency and reliability of the network questionnaire was analysed using Cronbach's alph (Cronbach 1951) and it was found to be 0.65 which shows good reliable questionnaire for this research study*

1. Introduction

INTRODUCTION

A network is defined as any set of interlinking lines resembling a net such as a network of roads [1]. A definition of security is given by The American Heritage Dictionary which states that security is freedom from risk or danger which insinuates safety and the network security is defined as the level to which a device or a program is safe from unauthorised use.

Data security and network security differ in their function. Data Security is the process of [1]transforming the client's data into cryptic data for transmission while the subsequent step is to decrypt the message. Most companies use MS SQL, MySQL as database technologies (See Figure 1).

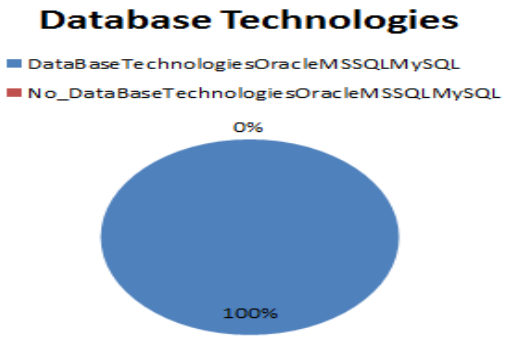
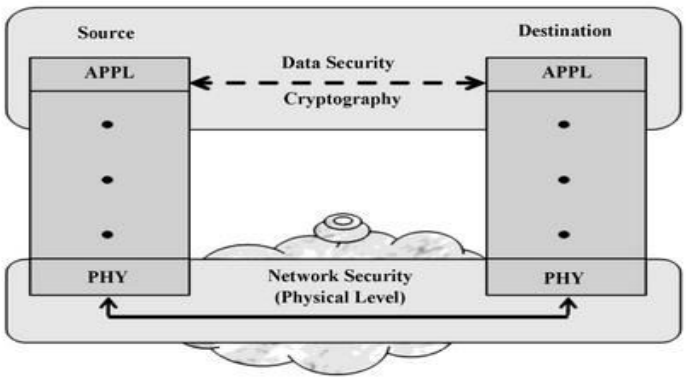


Figure 1: Database Technologies (Oracle, MySQL and MS SQL)

Currently, cryptographic methods are easy to break while further research should investigate on the development of unbreakable cryptographic methods. But cryptic messages transferred in the network can be protected by improving the security of the network (see fig 1). Cables, radio waves, telephone lines, satellites and infrared light beams are common ways that link computers in a network.

Fig. 1: Difference between Data Security and



Network Security (PHY means Physical layer and APPL means Application layer)

Network Security grabbed huge attention after Kevin Mitnick committed a computer-related crime in the USA causing losses of several million dollars [20, pp.118]. Network security has turned out to be essential to PC clients, associations, and the military. The rise of the internet years ago brought also a threat to the security [2]. The internet structure itself has permitted plenty security threats to materialise. But when modified, it can lessen various dangerous attacks that can be sent across the network. Before implementing proper security prototypes, we need to know how the systems are being hacked or attacked. Even though nowadays lots of security methods exist and can be easily implemented in the emerging networks, there is a lack of utilising them. Numerous organisations secure themselves from the web by employing firewalls and encryption instruments.

1.1 IMPORTANCE OF NETWORK SECURITY

The number of hackers recently is growing fast. For example based on responses from ten companies, one company claimed it has been hacked or its network security has been compromised (See Figure 2b). For this reason, the network needs security against them. Network security is made up of data security to prevent from unauthorised access and computer security. Network security should be considered important, as the damage done after a attack breaks it, compromises personal information and consume time by reinstalling the operating system and reestablishing information [20, pp.118]. Also based on responses of ten companies, it was noticed that 1 company stated that its security was compromised and four of the companies chose not to answer this question while the remaining responded that their network security was not compromised so far. So there is good reason to investigate how to improve the network security to curb the network attacks or intrusion of hackers even 80% of the companies claimed that they currently have intrusion detection system (See Figure 3c) In addition to that the companies used mostly Symantec antivirus licensed as well as Avira antivirus and Kaspery antivirus. Most companies claimed that they use VPN for remote access connections and therefore importance of network security should be emphasized at this level also.

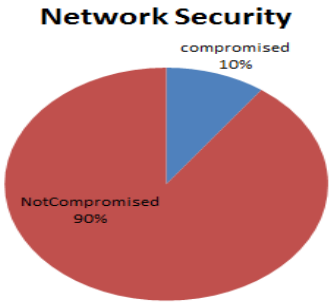


Figure 2: Percentage of companies or organizations whose Network Security has been tampered

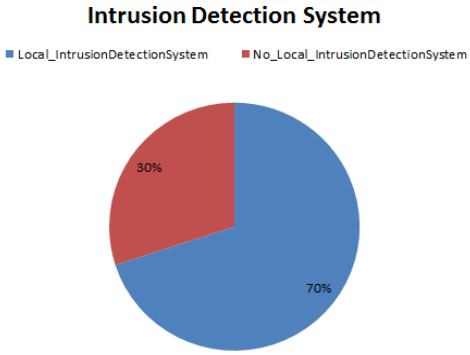


Figure 3: Percentage of companies who have local intrusion detection system.

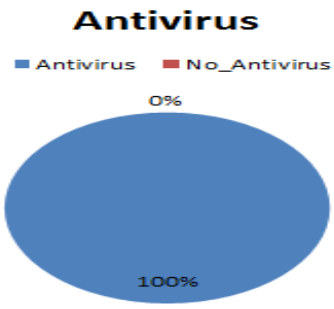


Figure 4: Percentage of companies who use antivirus (all of them) and these organisations are aware of the importance of antivirus.

In the incoming section we discuss various types of network security attacks and their impact on personal data, organisation and national security. We will also provide data obtained from ten various companies or organisations in Libya.

2. Open Systems Interconnection (OSI) MODEL

The Open Systems Interconnection (OSI) model, first approved in 1984, is an INTERFACE between the sender and the receiver. The purpose of implementing the OSI model was to remove the network complexity and to establish easy network

troubleshooting [21]. Fig 2 below describes the OSI model.

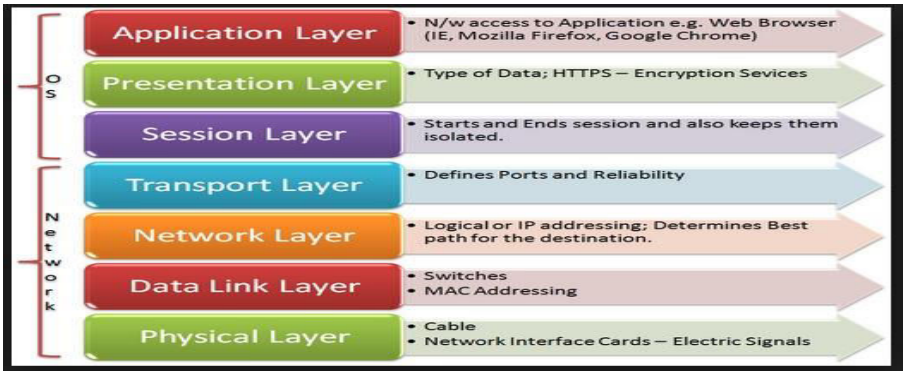


Fig 2: Open Systems Interconnection Model

Advantages

a. It gives an assortment of decision

b. OSI does not depend on a particular PC framework.
c. It gives encryption to information security
d. Multiple-system models can be included effortlessly.

Disadvantages

- Complex to implement
- OSI model is not adapted at all to telecommunication applications on computer
- OSI model demands agreement between users and service supplier.

3. CURRENT NETWORK THREATS

A. EAVESDROPPING ATTACK

Most of network communications happen in an unsecured format, which gives an attacker, who has secured access to data paths in your network, the power to "listen in" or decipher the traffic. Recently, wireless sensor networks (WSNs) are the primary focus of the business and academic research [5]. WSNs have been utilised generally as a part of ecological observing, social insurance, observation security and farming. Wireless nodes in the WSNs, situated in the transmission orbit of the transmitter can decipher the data when the transmitter and the recipient are unaware of the reconnaissance [6]. The eavesdropping attack is generally known for its critical security threat to a WSN (wireless sensor network). Needless to say eavesdropping attack is a necessary condition for other attacks to occur. Conventional WSNs contain wireless nodes furnished with Omni directional antennas. These types of WSNs transfer radio signals in all kinds of directions and unfortunately may be vulnerable to the eavesdropping attacks [4]. Investigators speak of two types of eavesdropping attacks in WSNs [7]:

(i) Passive Eavesdropping: In this type the malicious nodes discover the information by listening to the message transmission in the broadcasting wireless medium.

(ii) Active Eavesdropping: Here the malicious nodes act as friendly nodes and so archly receive the information via sending questions to transmitters.

Compared with the above mentioned Omni directional antennas, directional antennas work by concentrating radio signals on desired directions. For this reason there will be no weak signal in unwanted course. Thus, we conclude that directional antennas in WSNs can potentially reduce the interference [4].Furthermore directional antennas in WSNs [4] can improve the network performance.

B. SPOOFING

Spoofing stands for imitating another person or computer. This is often done by supplying false information: such as E-mail name, URL or IP address [8]. There are a variety of methods of spoofing. We would like in this paper to introduce and explain the following types:

1. IP Spoofing

IP spoofing is practically and universally used to gain unauthorised access to a computer. First the attacker delivers packets to a computer with a source address which implies that the packet comes from a trusted port. In order to accomplish the task and win the battle with the security, attackers must go through some perplexing steps [9]. They must:

- Secure a target.
- Getan IP address of a trusted machine.

- Deactivate the communication of the trusted machine (e.g. SYN flooding).
- Testa communication between the target and trusted hosts.
- Guess the sequence numbers of the trusted machine.
- Change the packet headers to give the impression that packets come from a faithful host.
- Attempt connection to an address authenticated service or port.
- If all above steps are successful, the attacker will plant for sure.

2. ARP Spoofing

ARP stands for Address Resolution Protocol. ARP has been used to portray IP addresses to hardware addresses. An ARP cache works by keeping a relation between each MAC address and its corresponding IP address. Just after an incoming packet (sent to a host machine on a network)arrives at a router, it requests the ARP program to find a MAC address that coordinates with the IP address. The ARP program will inspect the ARP cache and, if it finds the address, will provide it so that the packet can be converted to the right packet length and format and sent to the machine [9].

Thus, Spoofing counts in fabricating fake ARP request and reply packets. The process of sending fake ARP replies could convince a target computer to direct frames to computer B instead of sending to computer A. At the end of all this we could undoubtedly say that we have carried a ARP POISONING. Currently programs that deal with ARP poisoning are: ARPoison, Ettercap, and Parasite.

3. E-Mail Spoofing

An E-Mail Spoofing happens when an e-mail message appears to come from a legitimate source, but in fact it arrives from an impostor. The purposes behind E-mail spoofing are: viruses spreading, searchingfor sensitive business data and other industrial espionage activities.

4. Web Spoofing

All spoofing methods have to do with one simple duty: giving false information to victims. The Web Spoofing attack allows someone totally to scan and modify all web pages sent to a subject's device. Attackers can observe any kind of information that is inserted into different forms by the victim. From this point of view, because of the nature of the information the danger is quite alarming. Information could consist of: addresses, credit card numbers, bank account numbers, and the passwords that access these accounts. The attack can be devised using JavaScript and Web server plug-ins. It works in particularly two parts. First of all, the attacker must generate a browser on the victim's machine, with some identical-looking components supplied by the attacker. In the second phase the attacker brings about all Web pages destined for the victim's machine to be easily forwarded to the attacker's server. On the attacker's server, the appearance of the pages does not change too much. They can be read without difficulty. At the same time any actions executed by the victim (such as clicking on a link) would be registered by the attacker [9].

5. DNS Spoofing.

DNS spoofing attack can be interpreted as the successful insertion of incorrect resolution information by a host that in fact has no authority to provide that information. Techniques used to orchestrate the attack range from social engineering through to exploitation of vulnerabilities within the DNS server software itself.

The Packet Filtering is the best method to avoid various spoofing attacks. In this section we have described three packet filtering methods which are used to filter the spoofed packets, and they are :

a. Ingress Filtering Method – IFM

The technique of Ingress Filtering works by checking the relevance of the incoming packets, by ensuring if the packets come from the networks they declare to be from. In this method, packets coming into the network are filtered, if the network which send the packet is not allowed to do that.

b. Egress Filtering Method – EFM

Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

c. Spoofing Prevention Method –SPM

This comprises a novel method and it enables routers closer to the destination of a packet to verify the authenticity of the originlocationof the packet. In contrast to the standard ingress filtering, this method is effective mostly at routers next to the source.

C. DENIAL OF SERVICE (DoS) ATTACK

The Internet currently connects millions of computers around the world that are running on different software and hardware platforms. Every day, our lives are becoming more and more dependent on the Internet's services. There are numerous daily tasks that we rely on the Internet. In addition day to day new users are contributing to the Internet's growth. In this demanding environment, it is crucial to maintain correct operation, availability and security of the Internet services. Not only this high connectivity enables us to develop useful applications, but it also offers excellent chances for malicious users to engage and misuse computers all over the world illegally[10].

Denial of Service attacks constitute one type of these malicious activities. DoS (denial-of-service) attacks do not aim to alter data or gain unauthorised access, but instead they aim to disable applications, servers and whole networks. The attacker either utilises some vulnerability in a target network, or he misuses many compromised machines to send huge traffic to the target. The denial of service impact is made by the aggressor's movement meddling with an objective's operation, which makes it crash, hang, reboot or do futile work [10]. Two ways are to launch Dos attacks: one is from a single source and the other is from multiple sources. The second ones, the multiple-source DoS attacks are called distributed denial-of-service (DDoS) attacks.

According to Markova et al. [15] DDoS attacks are boosted sort of Do Sattacks. Attackers engage themselves to address hundreds or even thousands of compromised hosts called zombies against a single target. These zombie hosts are innocent computers who have no idea that they have been recruited for attacking by the attackers. After the final shock, the servers may be severely damaged. Now based on a short survey 60% of the companies use Microsoft window servers while the remaining use UNIX servers (Figure 5).

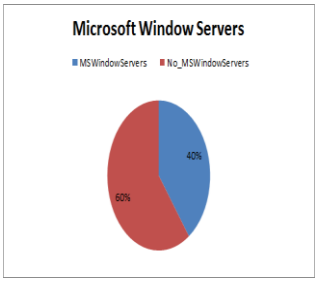


Figure 5: Percentage of companies utilising Microsoft window servers.

Due to the DDoS attacks the development of new Internet services may be impossible to implement. Network-DDoS are performed at the network layer. ICMP flooding, SYN flooding and UDP flooding are pure examples for Net-DDoS attack. Net-DDoS attack has all the power to exhaust entire network bandwidth so that the targeted host will either provide limited services, or provide services to only some users, or will not provide any services to its authorised users.

We have to say that attackers are furnishing themselves constantly with innovative techniques to break the network security. But the experts, who stay in the forefront of defensive effort, are not in the same past condition. Nowadays attackers face difficulties in launching DDoS attacks based on network layer. This because the amount of work that has been done by researches in this area to detect and block the Net-DDoS attacks is accomplished. However, attackers will relocate their a abusive strategies to application-layer attacks by building a more highly developed type of DDoS attacks , when a simple Net-DDoS attacks will fail [16].

Both DoS and DDoS offer a great threat for online services. But predominantly DDoS attacks are more difficult to handle because their traffic can be made highly similar to the legitimate traffic.

Service Interruption have immense financial consequences to organizations for services that are given online. For instance, if an online bank becomes inaccessible for 2 hours, this could end in losing customers, prestige and reliability due to a damaged reputation, over a long time.

DDoS attacks represent a devastating threat to network security as they impede network usage and additionally cause considerable harm[16]. Researchers have been inspired by the devastating negative impact of the DDoS in the life of many people and in the future of the business. There are taking more responsibility to understand and learn the techniques of the DDoS attacks. They are conducting investigations and simulation attacks in order to develop feasible and effective countermeasures against attacks. The main difference between DoS and DDoS attacks is stands in the fact that DoS attacks require one attack machine (to generate malicious traffic) while DDoS attacks employ a large number of attack machines.

There are four different ways to defend against DoSattacks**[10]**:

a. AUTHENTICATION

Passwords since the entry in the information security have been providing security mechanism for authentication and protection services against unwanted access to resources. Recently, lots of effort has been made to implemental graphical password. It is promising alternative of textual passwords. In the field of human psychology, it is said that humans are able to remember pictures easily. Graphical passwords not only improve the global security but also may avoid DDos attacks.

b. ATTACK DETECTION

Attack detection focuses the effort to detect DoS attacks in the process of an attack. It is an important procedure to direct any further action. The question is how to detect every attack as quickly as possible, without misclassifying any legitimate traffic? Here we are using dot defender a web application firewall for filtering the legitimate traffic against DDoS threats.

Attack Detection is a strong mechanism which stops the emerging attacks and so it prevents the damage from happening. Dot Defender web application firewall can avoid DoS attacks, by investigating the HTTP traffic and checking their packets against rules such as to allow or deny protocols, ports, or IP addresses[10].

The reasons why dot Defender offers such an astonishing security to the web are as following:

- Easy establishment on Apache and IIS servers.
- Strong security against known and developing hacking assaults.
- Best-of-breed predefined security rules for moment assurance.
- Interface and API for dealing with different servers effortlessly.
- Requires no extra equipment, and effectively scales with your business.

c. ATTACK SOURCE IDENTIFICATION

The pure intention of the Attack source identification is to locate the attack sources regardless of the spoofed source IP addresses. It is a crucial step to minimise the attack damage and it even provides a defense to potential attackers. The challenge that arise for attack source identification, is finding the way how to locate attack sources quickly and accurately without changing current Internet infrastructure. The greatest devastation brought on by the assaults incorporates: the consumption of the application service resource at the server side and the inaccessibility of administration access to real client. The last one poses a fatal system error which obligate “server rebooting” for full recovery. In the end we assume that any malicious behaviour can be discovered by monitoring the service resource usage, based on dynamic value thresholds over the monitored objects.

d. ATTACK REACTION

The solely purpose of the Attack reaction is to eliminate the effects of an attack. It is the final step in defending against DoS attacks, and therefore it conditions the real performance of the defense mechanism.

The devastating effects of the DoS and DDoS attacks have grab the attention of scientists and researchers, leading to various mechanisms that have been proposed to deal with them.

However, most of them have been proven to be non-successful when facing massively distributed DoS attacks. One way to better defend against distributed DoS attacks is taking into consideration to employ MDADF scheme (Marking-based Detection and Filtering) [11].

The MDADF plan utilises a firewall at each border routers of the network to be protected and the firewall examines the checking field of every single approaching packet to specifically filtering out the attack packets. On utilising our stamping plan, when a packet reach its destination, its checking depends just on the way it has navigated. If ever the origin IP address of a packet is actually spoofed, it is sure that this packet must have a marking to be distinguished from that of a true packet arriving from the same address. In the end, the imitated packets can be easily recognised and excluded the filter. Only the legitimate packets that carry the correct markings are welcomed.

1. Learning phase

In order to differentiate the spoofed packets, the firewall (See Figure 6)must have a record of the true markings. In the absence of the attacks the firewall learn and memories the correct markings for packets coming from specific IP addresses. The (IP-address, Marking) pairs are deposited in a Filter Table1. Later they are used to validate each incoming packet and if needed to filter out imitated ones. The learning phase continues for a sufficient time to allow most of the filter table to be filled up. If the Filter Table gets full, any new entry to be added replaces the oldest one.

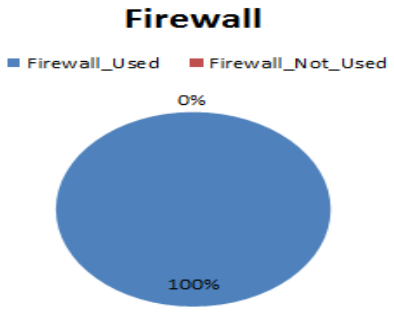


Figure 6: All organisations and companies recognize the importance of firewall. All ten companies have firewalls installed in their network system.

2. Normal Filtering Procedure

The action of the Firewall to filter out spoofed packets begins after the learning phase is accomplished. A Packet coming from an IP address and recorded in the Filter Table, it will be accepted if it has a stablemarking.On the other hands, it will be expelled.

3. Marking Verification

To confirm the markings in the Check-List, an arbitrary reverberation message is sent occasionally to the source address for every (IP-address, Marking) pair in the Check-List, and a counter is utilised to record the quantity of reverberation messages have been sent for it. To maintain a strategic distance from the answer being imitated by the assailant, the substance of the reverberation message is recorded in the Check-List and contrasted with the substance of answer got. On accepting a reverberation answer from the source, the stamping can be confirmed and the (IP-address, Marking) pair is moved to the Filter Table; else, it demonstrates the already got bundle was mock, then this pair is erased from the Check List.

4. Attack Detection

To detect the start of a DDoS attack, we use a counter called Total-Mismatches-Counter (T MC), which counts the number of packets whose marking cannot be matched at the firewall. For example packet with wrong markings as well as packets from unknown source addresses that are not recorded in the Filter Table. When the T MC value becomes greater than a threshold θ, it is considered as a signal of DoS/DDoS attack. The value of T MC is reset to zero after fixed intervals to ensure that the cumulative results over a long duration is not considered as the indication of attack by mistake [11].Whereas, defensive mechanisms against "Application Layer DDoS attack requires the following : (a) Access Matrix and (b) Hidden Markov Model [17].

D. SNIFFING

Sniffing is a typical system security assault in which a gadget takes critical data from the network traffic of particular network. The focus of the Sniffers are : passwords, files (FTP files, E-mail files), and E-mail text. Sniffing is an attack on confidentiality of data. The goal of sniffer is to find out the password and other personal information of the user. This action do harm to the confidentiality. Confidentiality is major challenge for the attackers on the internet In the air a large amount of data are travelling, and this amount has become a target for the attackers. They sniff for important data and use them for their interests. Different sorts of sniffing are as follows:

1. Client Side Sniffing

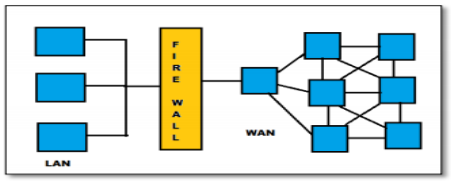
In this sort of sniffing the site page of sniffer uses programming dialect, for example, Java script deciphered by client operator sent to web servers. This technique is temperamental.

2. Server Side Sniffing

This kind of sniffing uses correspondence convention known as http. Sniffer assaults from server side.

3. Browser Sniffing

It is an attack in which websites are used and web applications in order to determine the web. This gives the emerging of various malicious activities like misinterpretation of HTML, cascading style sheets, etc. A network becomes by doing so a subject of stealing private information by a malicious. The internet serves itself free sniffer software, they can download from it and then install it in the computer. Sniffer changes their Network Interface Card (NIC) into unbridled mode, which gets bundles and passes it to framework piece. Sniffer shows these packets on programmer's PCs. Programmers keep up a record by taking a gander at network of users. Sniffing assault is exceptionally hard to distinguish furthermore it is difficult to overcome such sorts of assaults. In the world there are few researchers able to detect sniffers by two methods like ARP detection and RTT detection [13].



4. Content Sniffing:

In cheery sniffing, sniffers may change both the pattern and the content of the file. Content sniffing is also called as media type sniffing. This attack alter the true format of the file and the changed file hold a malicious content. Customisation of the content of the browser option is a simple way to get rid of this

attack. This sort of attack injures the client and server atmosphere [14].

5. Password Sniffing:

Sniffing attack destroys the confidentiality of the network security. The main objective of sniffers is to crack passwords and login information of the victim. The passwords are spared in packets and later uncovered to assailants. The best answer for arrangement against password sniffing is to utilise information triggers which control the estimation of the passwords.

6. Bots and Botnets:

Bots are computer program that offers various commands and control the system with the help of various kinds of protocols like- HTTP, FTP, Peer-to-Peer protocols. Bots which work on control instructions comprise Botnet. Botnet is a unique combination of robot and network. When a botnet is put in action this means the detruction of the computer system. Botnet attacks the computer networks without the knowledge of the victim. And they are a sophisticated technique deployed by attackers[14].

[4] FIREWALLS

A. DEFINITION

The thought of a divider to keep out gatecrashers goes back a large number of years ago. More than two thousand years prior, the Chinese manufactured the Great Wall as security from neighboring northern tribes. European rulers fabricated castles with high walls and canals to secure themselves and their subjects from attacking armed forces and from marauding bands. "Firewall" has been used in 1764 to outline some kind of walls used to isolate parts of a building, most likely to have a fire [18].In this paper we define a firewall as an assembly of devices between two networks, which meets these stand arts[18] :

• The firewall issituated at the dividing line of the two networks;
• There is no exception, the traffic between the two networks should go through the firewall;
• However, a firewall may allow some traffic to pass and block others (we call this process “filtering”).

A Firewall [19] is a networking system that helps us in preventing unauthorised access of one’s computer over the internet (ie, It acts as a protection barrier between the system and the network). It must be said that a Firewall can authorise both software and hardware appliances.

Fig. 3: A firewall system between LAN and WAN

All ten companies who provided responses for firewalls state that they have firewalls in their system to enhance network security.

1. Implementation of firewall in DMZ Environment

In Computer networks, a DMZ [19] is a demilitarised zone or a neutral zone that is in between a company’s private network and the outside public network. In the figure below the Main Firewall provide the access control and protection to the server from being hacked from the public network. A DMZ constitutes a more safe approach to a firewall and may excellently works as well as a proxy server.

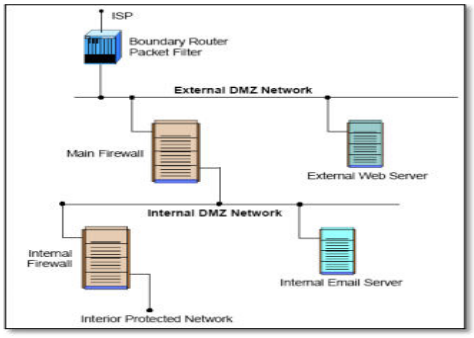


Fig. 4: Implementation of DMZ

2. Implementation of firewall in VPN

A Virtual Private Network (VPN) [19] is a private network that uses public network to connect remote sites or users together. It is clearly shown based on responses of various organisations that they all in fact utilize remote access services (See Figure 7).

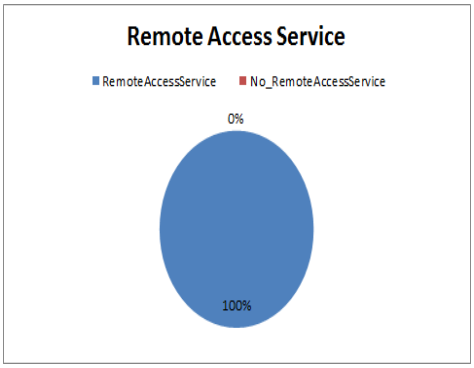


Figure 7: Remote Access Services by the companies

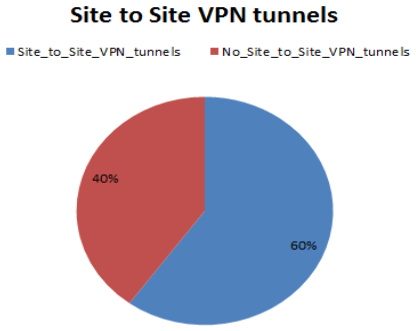


Figure 8: Percentage of companies which have Site to Site Virtual Private Network tunnels

The design of VPN comes by setting up a virtual point-to-point through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. The VPN firewall makes sure that the encryption of the systems is achieved successfully. It also prevent other users except legitimate users to access the network.

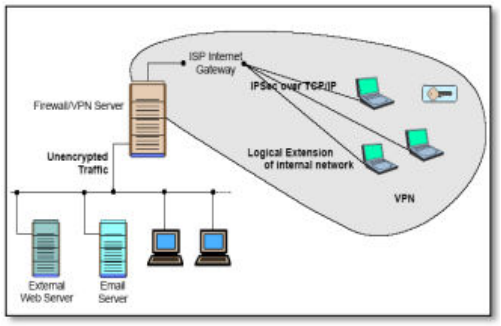


Fig. 5: VPN Implementation

3. Implementation of firewall in Intranet

An Intranet is a network that utilises the same sorts of service, applications and conventions that are available in a web, without outside connectivity. The Firewall ensures the intranet by checking the activity stream from the interconnected intranets.

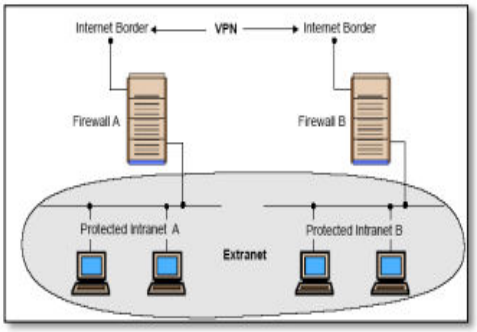


Fig. 6: Firewall Implementation in Intranet

4. Implementation of Firewall in Extranet.

Extranet is usually a business to business intranet. The Control access is provided to the remote user based on the authentication and authorisation as provided by a Virtual Private Network (VPN).

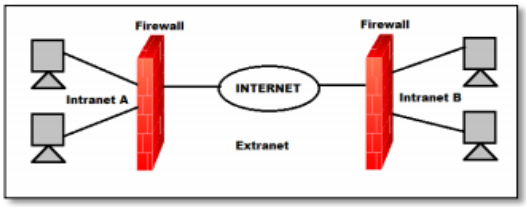


Fig. 7: Implementation in Extranet

B. TYPES OF FIREWALLS

Firewalls are broadly classified into four categories:

1. Packet Filters

The Packet Filters [19] firewalls work at the system level of the OSI model. Every packet is contrasted with an arrangement of criteria before it is sent. Packet separating firewalls is ease and has low effect on system execution.

2. Circuit Level Firewalls

Circuit level firewalls work at the sessions layer of the OSI model, or the TCP layer of TCP/IP.

3. Application Level Firewalls

Application level Firewalls [19], likewise called intermediaries are like circuit-level doors aside from that they are application SPECIFIC that is the portal that is arranged to be a web intermediary won't permit any File Transfer Protocol (FTP), telnet or other activity through.

4. Stateful Multilayer Firewalls

Stateful multilayer firewalls [8] offers a mix aspects of the other three types of firewalls. They filter packets at the network layer, figure out if session bundles are real and assess substance of packets at the application layer. Firewalls will keep on advancing as the assaults on IT industry and foundation turn out to be increasingly refined. Firewalls that sweep for infections as they enter the system and a few firms are right now investigating this thought, yet it is not yet in wide utilise.

REFERENCES

[1]Curtin, M. "Introduction to Network Security", http://www.interhack.net/pubs/network-security.

[2] Bhanu, Abhishek, Bhuvnesh,Akhil, 2014. Network Security, International Journal of Research in Information Technology, Volume 2, Issue 9, Pg. 185-194.

[3] Kartalopoulos, S. V., 2008. "Differentiating Data Security and Network Security," Communications, 2008.ICC '08. IEEE International Conference on, pp.1469-1473, 19-23.
[4] Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi-Wing Wong, 2013. On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas, International Journal of Distributed Sensor Networks.Volume 2013, Article ID 760834, 13 pages.
[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, 2002. "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422.
[6] F. Anjum and P. Mouchtaris, , 2007. Security for Wireless Ad Hoc Networks, Wiley-Interscience, New York, NY, USA, 1st edition.
[7] L. Bao and J. J. Garcia-Luna-Aceves, 2002. "Transmission scheduling in Ad Hoc networks with directional antennas," in Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02), pp. 48–58.
[8] P. Ramesh Babu, D.LalithaBhaskari, CH.Satyanarayana, 2010.A Comprehensive Analysis of Spoofing.International Journal of Advanced Computer Science and Applications, Vol. 1, No.6.
[9] Daemon, Route, Infinity, 1996. "IP Spoofing Demystified", Phrack Magazine.
[10] G Dayanandam, T V Rao, S Pavan Kumar Reddy, and RavinuthalaSruthi, 2013. Password based scheme and group testing for defending DDOS attacks. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3.
[11] Yao Chen, Shantanu Das, PulakDhar, Abdulmotaleb El Saddik, and AmiyaNayak, 2008. Detecting and Preventing IP-spoofed Distributed DoS Attacks. International Journal of Network Security, Vol.7, No.1, PP.70–81.
[12] AnubhiKulshrestha, Sanjay Kumar Dubey, 2014. A Literature Review on Sniffing Attacks in Computer Network.International Journal of Advanced Engineering Research and Science (IJAERS), Vol-1, Issue-2.
[13] Z. Trabelsi, H. Rahmani, K. Kaouech and M. Frikha, 2004."Malicious Sniffing Systems Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), 0-7695-2068-5/04.
[14] S. Pandey and A. S. Chauhan, 2013."Secure Content Sniffing for Web Browser: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 9.
[15] C. Chang, 2002."Defending Against Flooding-Based Distributed Denial of Service Attacks: A Tutorial," Computer Journal of EEE Communication Magazine, vol. 40, no. 10, pp. 42-51.
[16] Y. Xie and S. Z. Yu, 2009. "Monitoring the Application-Layer DDoS Attacks for Popular Websites," in Proc. Networking,IEEE/ACM Transactions, pp.15-25.
[17] Sreeja Rajesh, 2013. Protection from Application Layer DDoS Attacks for Popular Websites.International Journal of Computer and Electrical Engineering, Vol. 5, No. 6.
[18] Kenneth Ingham, Stephanie Forrest, 2002. A History and Survey of Network Firewalls.
[19] SahithiDandamudi&TarikEltaeib, 2015. Firewalls Implementation in Computer Networks and Their Role in Network Security. Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2, Issue 3.
[20] Dileep Kumar G., Manoj Kumar S. &Jyanthy M.K, 2016. Network Security Attacks and Countermeasures.IGI Global.
[21] Gaurav Bora, Saurabh Bora, Shivendra Singh, & Sheikh MohamadArsalan, 2014. OSI Reference Model: A Overview. International Journal of Computer Trends and Technology (IJCTT) –volume 7, number 4.
[22] Cronbach1951 http://www.psychometricsociety.org /sites/default/files/cronbach_citation_classic_aip_ha.pdf.