International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Network Security Mechanism Based On Static Internet Protocol Addressing

Ahmed D. Asad

Ahlia University, Department of Telecommunication Engineering, Manama, Bahrain

Abstract: ***Network security has become essential for computer end user, public and private organizations and also governmental defense authority. The whole field of network security is in a transformation stage and the wide topic of network security will be analyzed in term of a brief history of networking and security issues in the current rapid developing and challenging technological changes. This study aimed to design a security mechanism that is able to minimize the level of threats and unauthorized users over the network by utilization of static internet protocol features and aspects. In addition of providing the protection against data loss and prevented access to the network resources by the authorized user and network administrations.***

Keywords: Network security, IP implementation, Computer network, IP address, Threats

1. Introduction

Network security has become essential for computer end user, public and private organizations and also governmental defense authority. By the coming of internet, network protection and security twisted into a noteworthy concern. The historic background of network security allow a greater understanding of network security innovation and technologies. The network configuration in the current stage allow numerous security attacks and threats to happen. When modifying the current internet architecture it can work on reducing the possible threats by knowing the assault techniques and methods allow the network engineers to develop the proper security methods. Network security includes all activities that association, ventures and organizations embrace to ensure the protection of data and integrity of operation.

The whole field of network security is in a transformation stage. The wide topic of network security will be analyzed in term of a brief history of networking and security issues in the current rapid developing and challenging technology changes. Moreover this study will discuss the basic IP address types and versions and will give an illustration on the common network security attacks. Furthermore it will analyze the algorithm supporting the key generation of Static IP and explain some proposed example to show the security level of Static IP. Finally the study will also show typical methods to enhance the security of the current Static IP implementation. [1]

2. History of Network Security

The interest for network security was filled by the crime committed by Kevin Mitnick. Kevin carried out the leading PC associated misconduct in U.S. history. This action caused the USA to loss 80 million dollars due to misfortunes in intellectual property and foundation codes as of a range of companies. From that point forward, information protection originated into highlight. Because of Kevin crime organizations are underling security for licensed innovations. The main component of the network which is the Internet Protocol, were developed in the past without being able to provide security. This leaves the web open to threats and assault attacks. Current improvement in the Internet structure have made the internet connection more secure and with higher degree of data protection.

3. Secure Network

Framework and network innovation is key element in the technology for a wide assortment of user and in many applications. Security is critical to end users and applications. Despite the fact that, there is huge absence of security approaches that can be applied. At the point when bearing in mind system and network security it must underline that the entire network system is secure. Network security does not just concern the security in the end users devices, it should also consider securing the data transmission and connection medium against possible attacks that targets them. A convincing network security design is produced with the intellectual capacity of security issues, possible attacks, necessary level of security and variables that create a network powerless in contrast to assaults. However the following consideration should also be taken in mind when developing a secure network model: [1]

- Access: Approved and verified users are given the access to the network.
- Confidentiality: Data in network system keep being protected and private from other.
- Integrity: Guarantees the message has not been altered in transmission.
- Authentication: Guarantees the client identity that are using the network.
- Non-repudiation: Guarantee that the client does not discredit the use of the network and related services

4. Internet Protocol Architecture

The Internet Engineering Task Force (IETF) have offered security instrument to support the different layer of Internet Protocol Suite. These security instruments take into account the consistent reassurance of data that are exchange over the network.

4.1 IPv4 Architecture

The IPv4 was introduced in 1980. The protocol consist of

two or three viewpoints which created concerns with its operation. These issues doesn't all classify under the security category. [1] However they are explained to pick up a far reaching understanding of the internet protocol and its drawbacks. The causes for the issues with the internet protocol are:

Address space and routing: The IPv4 construction modeling has address that is 32 bit long. This limits the greatest number of PCs that can be joined with the network. On the other hand, routing is an issues for this protocol in light the fact that routing tables are always expanding in size.
Security: the nonappearance of integrated security inside the IPv4 has driven numerous assaults. Instrument to secure IPv4 do exist. However there are prerequisite for their utilization. IPsec is particular mechanism that is used within the IPv4 to ensure the security. IPsec safeguards the transmitted packets by technique of cryptography and its encryption/decryption process.

Quality of service (QoS): As the network extends and innovation advanced, different types of data standard to be transmitted over the network. The QoS for sending and streaming the music and video files are vastly different than the standard data such as text. The protocol does not have the workability and functionality of the quality of service.

4.2 IPv6 Architecture

The IPv6 protocol has implantation to overcome the IPv4 drawbacks and limitations. At the point when IPv6 was being created accentuation was put on aspects of the IPv4 protocol that should have been moved forward and improved. The enhancement where placed in the following regions:

a) **Addressing and Routing:** The IPv6 protocol address was stretched out by 128 bits instead on 32bits used in IPv4. Moreover the IPv6 routing mechanism proficient and empowers smaller routing tables. [1]
b) **Security:** The security building design of the IPv6 protocol is superior. IPsec is installed inside the protocol itself. IPsec function exactly the same on both IPv4 and IPv6 but with the alteration that IPv6 can use the security system along the whole routing table. [1]
c) **Quality of service (QoS):** The quality of service issues is taken care of with the IPv6. The internet protocol works on providing a method to treat the specific packets with high level of quality of service taken in consideration. [1]

5. Internet Protocol Addressing

An IP address recognize a PC or Other devices of a network system. The fundamental concept is each device on a network system to have an address. This way, information is transmitted to the opportune spot. There are two main types of network IP addresses:

a) **Static IP Address:** When a network enable device is allotted a static IP address, it doesn't change. The IP Address will always remain constant.
b) **Dynamic (DHCP) IP Address:** Most Network enable devices use dynamic IP addresses, which are allotted by the DHCP server. These IP addresses are makeshift, and can change after some time, and producing the risk of reducing the level of network security because the attacker can perform IP Spoofing Attacks when Dynamic IP Address is in use.

6. Common Network Attacks

Internet attacks are separated into classification. A few attacks select the network system or data, for example: Eavesdropping and IP Spoofing attacks. Assault can likewise meddle with the network system and it functionality, such as worms, viruses and Trojans horses. The other type of attack select the system resources to use it and consume it performance uselessly, these can be done by denial of service (DoS) attacks.

6.1 Static IP Address and Spoofing Attacks

One of the issues with Dynamic IP Address is IP spoofing attacks which is overcome with the use of Static IP Address since it doesn't request the IP Address from a server or even generate any address from any source and instead it have a fixed address that will remain constant always which will positively ensure a greater level of protect and network security to end users and businesses.

In brief words to clarify the spoofing attack on (Dynamic IP Address), client computer using Dynamic IP Address is sending DHCP Request on the LAN network. This request is usually a broadcast and in some cases multicast in order to receive reply. And since this request is open to all the network host on the LAN everyone can listen to that request but only the DHCP server will understand the nature of the request. In turn DHCP server in then answer the client request with a message that it will provide it with configuration needed. These configurations are IP Address and Subnet Mask. However we have attacker on the network who will reproduce and simulate the DHCP server rule on his computer. With such activity he will have the right to reply the request done by the client computer before the real DHCP Server do that due that the attacker is closer in distance to the client than DHCP server. In this way, he will target all the communication of the client. Moreover he will make conceivable to forward the packets to the real destination, keeping in mind the end goal of allowing the client communication possible but with the ability of sniffing the packets and frames of the client computer in real time.

7. Methodology

7.1 Model 1: Secure communication based on Asymmetric Static IP Address

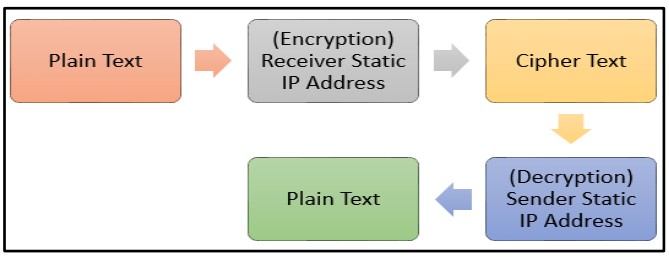

Figure 1: Asymmetric based on static IP Address

Cryptography

Network system and cryptography algorithms are ideas to ensure protection for our network and data transmit over remote network system. Information security is the most important goal of secure data transmission over problematic network. Data security is a testing issue of data communication nowadays. Accordingly, it is imperative to apply powerful encryption and decryption technique to improve data security. [2]

Asymmetric Algorithm

The algorithm calculate two keys, a public key and a private key to utilize them for encryption and decryption process. The public key is shared to all and each individual from the group have the unique private key for his own. Generally, the public key is used for encryption and the private key for decryption the received message. The pair blend of public and private key is exceptional. In the event that a public key is known to the others, they cannot decrypt the message in light of the fact that they don't have the opposite side of the decryption which is the private key. Asymmetric algorithm makes the public key encryption framework a highly effective and efficient cryptographic system. [3]

Key Generation using Static IP

As it was illustrated earlier the asymmetric algorithm uses two key for the encryption and decryption process. The key pair is based on a prime number of long and wide length. In this proposed model, instead of generating the keys using the prime number and the asymmetric RSA algorithm, we will replace the keys with the sender and receiver Static IP Address.

The distribution of the public and private keys will be as the following:

- Sender Static IP Address = Private Key which then will be used for the decryption process.
- Receiver Static IP Address = Public Key which then will be used for encryption process.

Each cryptography has four essential objectives, the Static IP using Asymmetric algorithm guarantees that the four objectives are met. [3]

Table 1: Objectives of the Static IP Using Asymmetric Algorithm

Privacy	Data must be protected from unapproved parties.
Integrity	Message must not be adjusted or modified.
Authentication	The process which the Sender and Receiver demonstrate and prove their identification to one another.
Non-repudiation	Confirmation is required that the send message was in reality received

7.2 Model 2: Email Security through Static IP Address and Biometrics

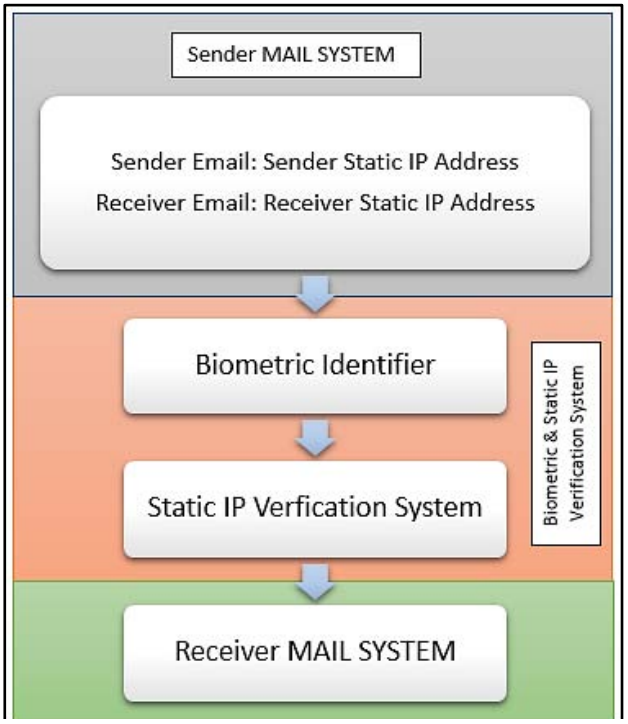

Figure 2: Static IP Email Security

The proposed Email Security Model will work on collecting the sender Static IP Address and the destination Static IP Address, then insert them through (Biometric Static IP Verification System) which has two components. [4]

The first instrument (Biometric Identifier) will work on verifying and confirming the identity of a person through physical estimation or behavioral characteristic. Since biometric identifiers are related to the user, they are more dependable and accurate than token cards or information based validation system.

The second component is a software based tool that work on verifying if the sender IP address is Static or dynamic by IP ADDRESS LOOKUP Services and then match it with a list of Static IP addresses in database. If both the person identification and the IP address is static, then the data will be received by the destination and can be viewed by that user.

Security Features Provided by the Proposed Model

Authentication – In the proposed model the verification of user identity is provided which proves that the email message and related attachments are received by the intended recipient.

Privacy – Any email messages that are not encrypted can be effectively captured and read. Attacker might be able to take a look on the Inbox or snatch the messages. The two stage biometric and Static IP Address verification framework permit the user to effectively encrypt emails and guarantee that message and related attachments are being used and read by the expected reception. [4]

Integrity – Talking generally, unsecure email messages can be faked. Messages can be created that look just as they were from a specific individual or company, but in fact they are from somebody totally obscure. Biometric identifier first checks to approve the person then move to the second stage where the Static IP verification is utilized to confirm that it is

incomprehensible for anyone to modify the substance of the user email message without they be notified for that action.

7.3 Model 3: E-Commerce Security Based on Static IP Address

Internet security has tuned into reliable and developing issues as new technologies being created. The number of security attacks and related episodes keeps on expanding. Protection control over personal information and security the endeavored access to information by unapproved others are two fundamental issues for both E-Commerce and on-line banking. Without either, purchasers won't visit or shop on-line, nor does using on-line banking service without considering both. [5]

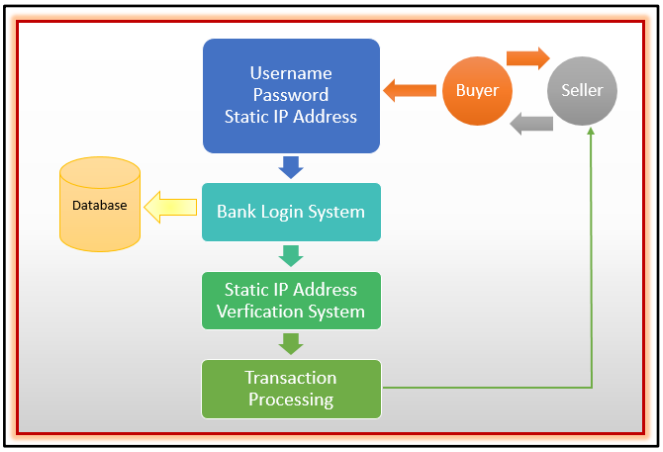

Figure 3: Static IP E-Commerce Security

In this proposed E-Commerce security model, the user is protected with new technique in term of identity verification. This method provides the user with enhanced network security level through double stage verification that work on 3 phases:

Phase 1: The user attempt to buy from an online seller and an electronic transaction must be completed in turn to set the online order. The proposed system model will ask the user to enter his/her username and password and with advance toolkit it will also identify the user Static IP Address automatically. However these personal details about the user were already filled by them previously and they have been saved on the bank database system.
Phase 2: The given details will follow the process of validation the username, password and their Static IP Address to ensure the identity of the user and prevent unauthorized access to the banking information.
Phase 3: If successfully the identification id verified, the transaction is then will process and a connection link will establish with the (Seller) registered bank account in order for the payment procedures to proceed.

Security Features of E-Commerce Model

The Static IP Address based E-Commerce will provide the following network security measures: [5]

- **Confidentiality:** The information is protected from attackers and unauthorized parties.
- **Authentication:** The buyer need to prove their identification over two stage system which will guarantees to limit the network attacks to maximum.

8. Importance of Static IP Address

Reaching to this point in analyzing the Static IP Address I can positively note that Static IP Address is a dependable and reliable method of addressing for services such as Voice over Internet Protocol (VoIP), and it is more solid to use with gaming consoles and media streaming hubs... etc. Static IP Address are likewise great if clients serves as server, which will results in faster download and upload speed than normal connection speed. In addition, Static IP Address is vital when hosting organization website or personal purposes website. [6]

9. Security Issue with Static IP Address

Static IP Address can turn into a security risk, because the fact that the address always remain constant and it way easier to TRACK the PC for accessing your data and information or taking control over your computer resources to use it for his desirable purposes such as attacking other computer within the organization in order to reach for the sensitive information that he wish to gain access to them.

10. Security Configuration to Enhance Static IP Address

In order to overcome the issue of Static IP Address which is mainly the possibility to easily TRACK a network enabled device by knowing their fixed IP Address and performing the network attacks methods. I have managed to design a security configuration that works on securing and protecting the network devices with Static IP Address assigned to them.

The designed model follows the most effective defense strategy available to secure networks. By using a Firewall it will decreases the risk related to Static IP Address to minimum. A firewall is a monitoring and control system that works to block the traffic activity from outside the organization network, yet it could likewise to be utilized to block the traffic activity from inside the organization network. A firewall is the forefront guard component to act against intruders and to prevent unapproved access to organization network resources.

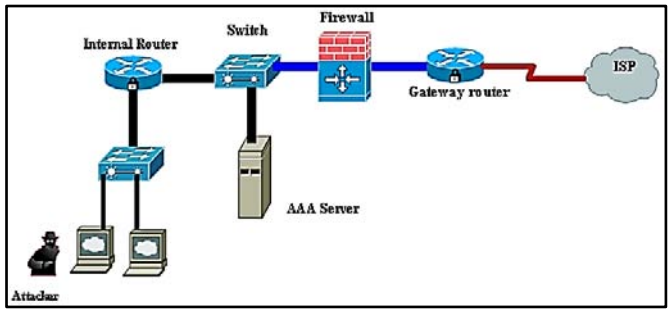

Figure 4: Firewall

11. Results and Findings

From the previous models analysis I have come up with the following findings:

- Static IP Address is a great option to overcome the issue of IP Spoofing attacks that is common to dynamic (DHCP) IP address. Since Static IP is constant and doesn't require to allocate the configuration from any server on the LAN network.
- Cryptography using asymmetric algorithm can provide more security level in encryption and decryption process when it is based on Static IP Address key generation. This ensure data is secure when transmitted and the right receiver is the only person who is able to decrypted and read the content of the data.
- Security measures in Email System can be enhanced to reduce the unauthorized access to the system by using two stage verification system which is based on Biometrics and Static IP Address. The system will work on protecting the clients from attacker and hackers.
- The security level of Static IP Address make it a decent method to be used in online banking services to replace the traditional authentication method that is implemented over username and password only. This satisfy that a higher degree of identity verification is assured.
- Static IP Address can serve as a superior security option for the network configuration when it is combined with virtual or physical based firewalls. This provides the end user with protection against tracking of data and controlling over network resources.

12. Future Trends in Security

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system.[1]

The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

13. Conclusion

Network security is an imperative field that is increasingly picking up consideration as the network systems expands. The security risks and internet architecture were analyzed to decide the fundamental security measures and innovation. The security innovation is mostly based on software, on the other hand numerous hardware like Firewall can be also used. Nowadays the overall activity of different association, companies and end users are through the network system.

The most vital security issue to consider when communicating is unapproved access. The objective of these assaults is to get to critical and profitable resources and information. Therefore network security plays an important rule to protect us from attackers and intruders. This study helps the network administration and also the end user to understand the risks associated with network and data privacy.

The critical part of this study is to prove that Static IP Address is a superior method of addressing and network technique to provide overall security measures to the network system. To sum up, the conducted research through data analysis and discussion of typical applications and network models that are in use with Static IP Address assure that network security is achievable using Static IP Address. Finally to enhance the security level of Static IP Address we have combined it with firewall to prevent the common issue of traceability. [1]

References

[1] B. Daya, "Network Security: History, Importance, and Future," University of Florida Department of Electrical and Computer Engineering , p. 13, 2013.
[2] J. E. Canavan, Fundamentals of Network Security, Artech House, 2001, p. 319.
[3] D. T. M.Jayakumar, "Static IP Address based Asymmetric Algorithms," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 1, no. 1, p. 4, 2012.
[4] D. T. M.Jayakumar, "E-Mail Security Through Static Ip Address And Biometrics-Token Card System," International Journal of Advanced Research in Computer Science, vol. 3, p. 4, 2012.
[5] T. M. Jayakumar, "E-COMMERCE SECURITY THROUGH STATIC IP ADDRESS," Asian Journal of Computer Science and Information Technology, p. 3, 2012.
[6] W. Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 2007, p. 413 pages.

Author Profile

Ahmed D. Asad received his B.Sc. degree in Mobile and Network Engineering from Ahlia University Bahrain in 2016. Since 2012 - present, he positioned his efforts and concerns in academic researches to fulfill the gaps in knowledge and upcoming technological and scientific challenges that may face the entire world and MENA region as specific.