An Insight to Network Securit

Aman Arora
Department of Computer Science
HMR Institute of Technology
New Delhi, India

Mantu Kumar
Department of Computer Science
HMR Institute of Technology
New Delhi, India

Shally Gupta
Assistant Professor
Department of Computer Science
HMR Institute of Technology
New Delhi, India

***Abstract*-Network Security is very severe problem nowadays. With the initiation of the World Wide Web and the emergence of e-commerce applications and social networks, organization across the world generate a large amount of data every day. One of the problems with mobile networks is the deficiency of security information of the networks. Unlike from organization and home networks, the security measures and situation of mobile networks are generally unknown to the end users. As a result, users may enter a mobile network bled with attacks without any past protection and suffer serious damages. Security is an important field that consists of the provisions made in underlying computer network infrastructure, policies adopted by the network administrator to protect the network, the network-available resources from unofficial access and the efficiency of these measures combined together. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts. This paper discusses the state of the art for a wider range of cryptographic algorithms that are used in networking applications.**

Keywords: Internet, Network Security, Firewall, Attacks, Threats, Phishing, DOS, Cookies;

I. INTRODUCTION

Network security is a challenge for network operators and internet service providers in order to prevent it from the attack of intruders. It deals with the requirements needed for a company, organization or the network administrator to help in protecting the network. Computers, networks, and the Internet affect our lives every day or we can say that we are so much dependent on them to make our life comfortable [2]. We all are connected to the internet without any boundary, so Network Security is essential in this environment because any organizational network is accessible from any computer in the world .Network Security can be referred as protecting websites domains from various forms of attack. If we have the knowledge of how various attacks are executed we can protect ourselves.Security means considering vulnerabilities, threats, attacks, countermeasures, and acceptable risks [2]. A Network were developed using different communicating devices. The Synchronous network consists of switches but do not require any security because switches do not buffer any data but anetwork consist of routers must be secure enough as information can be easily stolen by using malware like “Trojan Horse” [4]. Networks were developed so that we could share expensive computing resources. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. The terms, information security and network security are most of the time used to represent the same meaning. Network security, though, is more particularly taken as the stipulation protection from outside intruders. When accessing information in an internetwork environment, secure areas must be created. The device that separates each of these areas is known as a firewall. A firewall usually separates a private network from a public network.

II. RELATED STUDY

Problems in network security: All network face one or more issue, it is the responsibility of the network administrator to keep the network secure for malevolent software, worms, and threats and from other attacks. An attack is an information security threat through which the impostor attempt to obtain, modify, remove, implant or reveal confidential information without authorized access or permissions. Classes of attacks are [4] [7]:

A. Passive Monitoring of Communications (Passive Attacks)

In this attack the confession of the confidential information or the files to an attacker without the assent of the authorized individual or an organization. The attacker monitors for the open ports or vulnerabilities to gain the information about the objective without changing it on the target machine. There are two main types of passive attacks:

B. Active Attacks

In this type of attack the hacker try to make changes to the data on the target machine. It can be said as the attacker can modify the stream of bits or conception of false stream of bits but the goal is same and much more of the passive attack and that is to steal the private information of the individual or organization and also do harm to the networkor network services which they are providing. The active attacks are subdivided into different categories:

- *Replay Attack*: It is a breach of security in which the hacker can store the information and then retransmit it with a swindle to the receiver with some unauthorized operations such as false identification or a replacement transaction. Replay attack is also known as a "man-in the-middle attack," and It can be prohibited by using strong digital signatures which include time stamps and inclusion of unique information that will be different from the previous transaction like a value of a constantly incremented sequence number.

- *Masquerade Attacks*: The impostor pretends to be a particular user of the network system so that he can gain the access or some constitutional rights that the user is authorized for. This attack is attempted through the use of stolen login Ids and passwords. Modification of Messages: In this type of attack the intruder can use two different ways to modify the message either he will alter the packet header addresses to direct a message to a different destination or he will modify that data on the target machine so that an unauthorized effect can be produced. This is a very common type of attacks that issued.
- *Denial of Service (DOS):* It is very hard to prevent the occurrence of DOS attacks because of all the vulnerabilities of software, hardware, and the network. Here users are destitute of access to the network or its resources. The entire network is disrupted by overloading the messages than it can handle to mess up its performance. DOS are the major threat to network security in today's scenario because they can be easily launched with some basic knowledge.
- *Distributed Denial of Service (DDOS):* DDOS is a type of DOS attack where multiple compromised systems (Sometime called a botnet or zombie army), which are frequently infected with a Trojan horse, are used to target a single system causing a Denial of Service (DOS) attack.

C. Insider Attack

These attacks involve someone who has authorized access to the network with either a description on the server or having a physical access to the network. He can purposely or fortuitously attack the network from some malicious or non-malevolent ways malevolent insiders intentionally snoop steal, or damage the information and they can use this information in a deceitful manner. They can also deny access to other authorized users. In the same way attacks can be non-spiteful while performing the tasks in an organization like carelessness, lack of knowledge, or intentional circumvention of security. Internal interference Detection System (IDS) protects organizations against insider attacks.

D. Close-In Attack:

When an individual or a group is trying to attain close immediacy to networks so that, they can alter, collect the information or deny the access to the information. Close physical propinquity can be achieved through secret entry into the network or an open access

One of the popular close-in attacks is social engineering, where the attacker compromises the network through social interaction through an e-mail or over the phone. The attacker will apply some actions in the conversation so that the victim can disclose the secrets of the company and he attacker could put on unauthorized access to the network or to the system.

III. TYPES OF WEAKNESS

Network Security and Protection Security has one purpose, to protect resources. With the initiation of personal computers, LANs, and the wide open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, finding the stability between being isolated and being open will be significant. This technology gave businesses a balance between security and simple outbound access to the Internet, which was mostly used, for e-mail and Web surfing. Network security is the most essential component in information security because it is responsible for securing all information passed through networked computers [5] [6] must follow three fundamental precepts. On one side of the gateway is the internal network that must remain secure, and on the other is the information needed from the outside world combined with the unwanted threats of external networks. Three of the major types of firewalls, listed in order of increasing quality and price, are packet-filtering routers, application-level gateways, and circuit-level gateways. Although it is not the best available firewall, a positive step in increasing network security is the use of packet filtering routers.

A. *Weakness due to configuration:*Attacks on Router When discussing network security, three common terms used are vulnerability, threat, and attack. Vulnerability is a weakness, which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses. Configuration Weaknesses: Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

B. Security Policy Weaknesses: Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy[9][12] IP spoofing involves the capturing of the information in an Information Packet (IP) to obtain the compulsory address name of a workstation that has a trusted relationship with yet another workstation. In doing so, a hacker can then act as one of the workstation and use the trusted relationship to gain entry into the other workstation where any number of actions can be performed. Finally, E-Mail is extremely helpless and quite liable to a number of different attacks. Smurf Attack, this attack involves sending a large amount of ICMP echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. If a router is positioned to ahead broadcast requests to other routers on the protected network, then the router should be configured to avoid this forwarding from happening. This blocking can be achieved by denying any packets destined for broadcast addresses. Distributed Denial of Service (DDOS) Attacks, several high-profile DDOS attacks have been observed on the Internet. While routers and firewall, cannot prevent DDOS attacks in common, it is usually sound security practice to dispirit the activities of specific DDOS agents by adding access list rules that block their particular ports. But some of these rules may also inflict a slight impact on normal users, because they block high-numbered ports that lawful network clients may randomly select. Therefore, you may choose to apply these rules only when an attack has been detected. Otherwise, these rules would normally be applied to traffic in both directions between an internal or trusted network and an un-trusted network examples of denial of service attacks are (Ping of death, SYN flood attack, Packet disintegration and reassembly, E-mail bombs, CPU hogging, Malicious applets, Misconfiguring routers, The chargen attack, Out-of band attacks such as Win Nuke, Land.c, Teardrop.c, Targa.c, Masquerade/IP Spoofing).

C. Router and Firewall Security: Policy Routers perform many different jobs in modern networks, forwards traffic between two or more local networks within an organization or endeavor routes. Interior routers may impose some limitations on the traffic they forward between networks. Forwards traffic between different enterprises (sometimes called different 'self-directed systems'). The traffic between the different networks that make up the Internet is directed by vertebrae routers. The level of trust between the networks connected by a vertebrae router is usually very low. Typically, backbone routers are designed and configured to forward traffic as quickly as possible, without magnificent any restrictions on its[4]. Configuring backbone routers is a very specific task. The border router forwards traffic between an enterprise and outer networks. The key aspect of a border router is that it forms part of the frontier betweenthe trusted internal networks of an enterprise and un-trusted external networks (e.g. the Internet). It can help to secure the perimeter of an enterprise network by enforcing restrictions on the traffic.

Test Bed and Performance Testing In order to test the security and performance of the suggested network model, a test bed was make and establish. The test bed is consisted from the two Cisco router 2811, Cisco firewall (PIX) 516E, Cisco switch 2960, AAA server with TACACS+ protocol and two workstation work as real attacker and hacker. The following events were taken to examine the network operation to test the network security heftiness against different types of attacks. Also some scanning tools are used to simulate real network attacks and intrusions on the objective system.

IV. NETWORK SECURITY MODEL

A message is to be transferred from one party to another across some sort of Internet service. A third party may be accountable for distributing the undisclosed information to the sender and receiver while keeping it from any opponent. Security aspects come into play when it is essential or enviable to protect the information transmission from an opponent who may present a risk to discretion authenticity, and so on. Figure 1 shows the model of network security.

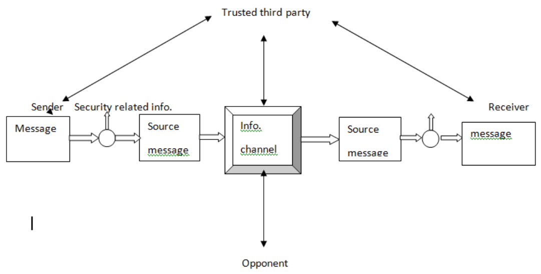

Figure 1: Network Security Model

All the techniques for providing security have two components:
(a) A security-related transformation on the information to be sent. Message should be encrypted by key in order to illegible by the opponent.
(b) An encryption key used in combination with the transformation to mix up the message before transmission and sort out it on reception.

A.Cryptography Mechanism: Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is projected can read and process it. The term is most repeatedly associated with scrambling plaintext message (ordinary text, sometimes referred to asclear text) into cipher text (a process called encryption), then back again (known as decryption). There are, in general, three types of cryptographic schemes typically used to achieve these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. Secret Key Cryptography Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. Block ciphers can operate in one of several modes: the following four are the most important: (i) Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a cipher text block. Two identical plaintext blocks, then, will always generate the same cipher text block even though this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks. (ii) Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively- O-Red (XO-Red) with the previous cipher text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same cipher text. (iii) Cipher Feedback (CFB) mode is a block secret message implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be helpful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the cipher text is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded. (iv) Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same cipher text block by using an internal feedback mechanism that is independent of both the plaintext and cipher text bit streams. Secret key cryptography algorithms that are in use today include data.

B. Encryption Standard (DES): DES is a block cipher employing a 56-bit key that operates on 64-bit blocks. DES algorithm as described by Davis R. [7] takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length.3DES (Triple DES) [3] is an enrichment of DES; it is 64 bit block size with 192 bits key size. In this regular encryption method is like the one in the original DES but applied three times to raise the encryption level and the usual secure time.

V. CONCLUSION

This paper deals with and discusses the security flaws in router and firewall configuration system and risks when linked to the Internet .Also this paper presented the guidelines and recommendation to achieve a best security and to guard the network from vulnerabilities, attacks, and threats by applying the security configurations on router and firewall. Also one can use this recommended security policy as a checklist to use in assessing whether a unit is adhering to best practices in computer security and data secrecy. This work appears the firewall provides supplementary access control over connections and network traffic and execute user authentication. Using a firewall and a router together can offer improved security than either one alone. A poor router filter arrangement can reduce the in general security of a network, depiction internal network components to scans and attacks. The existing definition of network anomaly reports an incidence that diverges from the normal behavior. However there are no recognized models accessible for standard network behavior. The proposed scheme introduces an substitute technique by using features selection like IP address of source and destination, port number of source and destination, packet size, packet rate and connection time to sense an attack. In addition it also decreases the false alarm rate thereby escalating the true positive rate. The major potency of the new scheme is that it can detect attacks that come with altered packet size. Experimental sample data set which we have taken is comparatively petite and hence this data-set would not cover all the attacks in the world. There are a lot of latest attacking methodologies introduced by the attackers nowadays. All the methods are not offered to the public due to security reasons, so it is difficult to study about the attack schemes and prevention mechanisms. Still a lot amount of data is presented for academic purposes.

Future Scope: In future this system can be extensive by using large data sample set and by incorporating as several major attacks possible also more precise threshold value can be found which can help in making the system more accurate. Research can be carried out in order to expand on cloud platform thereby making the system as a generic service provider.

REFERENCES

[1] Inam Mohammad, “A Review of types of Security Attacks and Malicious Software in Network security”, Vol.4, Issue5, May2014.

[2] BhavyaDaya, “Network Security: History, Importance, and Future”, 0University of Florida Department of Electrical and Computer Engineering.

[3] Vaclav Matyas, “Biometric Authentication-Security and Usability”

[4] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology,2004.

[5] Alabady S. , "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA’2008

[6] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[7] C. Cranor, T. Johnson, O. Spatscheck, and V. Shkapenyuk.Gigascope: A stream database for network applications. In Proc. of the 2003 SIGMOD Conf.,June2003.

[8] K. Xu, Z. Zhang, and S. Bhattacharyya.Profiling internet backbone traffic: Behavior models and applications. In Proc. Of ACM SIGCOMM,2005.

[9] D. Brauckhoff, B. Tellenbach, A. Wagner, A. Lakhina, and M. May. Impact of traffic sampling on anomaly detection metrics. In Proc. of ACM/USENIX IMC,2006.

[10] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred.Statistical Approaches to DDoS Attack Detection and Response. In Proc. of DARPA Information Survivability Conference and Exposition, 2003

[11] International Journal of Computer Applications (0975 –8887) Volume 62–No.15, January 2013 Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud A.S.SyedNavaz, V.SangeethaC.Prabhadevi [10] . Shannon. A mathematical theory of communication.Bell System Technical Journal, 27:379–423,July,1948.

[12] Dorothy E. Denning. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, 13:222232,1987.

[13] N. N. Wu, “Audit data analysis and mining”, Ph.D. Thesis, George Mason University, USA, 2001.

[14] Simmonds , A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323. doi:10.1007/978-3-540-301769_41. ISBN 978-3-540-23659-7.