Designing Optimized Architecture for Network Security Devices

Rohan Badlani

***Abstract*—Cyber Crimes are growing and it is expected that by 2017, the global cyber crime market would value at around $120 billion. It has been found that on an average, 18 users become victims of cyber crime. Viruses, Malware, Trojans, Worms, SQL injection and Phishing are some of the malpractices that take place on the network regularly. Many different approaches have been taken by Computer Scientists and researchers to combat this situation but still these malpractices happen to occur at an exponentially growing rate. This calls for the attention of Computer scientists to look for newer security systems to combat such software and hardware based malpractices.**

***Index Terms*—Firewall, Demilitarized Zone, Proxy servers, Packet filters, Application gateway, Bastion hosts.**

I. Introduction

An unstoppable growth of the networks from 1990's onwards has led to the origin a new field of crime called the Cyber Crime. Cyber Crime is an offensive act committed against an individual or a group of individuals with a motive to intentionally harm the reputation of the victim or to cause a physical or mental directly or indirectly using modern network such as the Internet and SMS/MMS over Mobile phones. It has been found that botnets have been using as many as 1,20,000 infected "zombie" computers to send out spam every day. In order to make the users of the network all over the world secure new researches are being carried out in the field of Intrusion Detection and Prevention systems that monitor network and system activities for malicious activity. Network Security is a technological mix of Hardware and Software components that detect an intrusion into unauthorized locations over the network and hence helps prevent cyber crimes over it.

Paper written on August 07, 2013; revised on August 15, 2013; This work was supported in part by the Birla Institute of Technology and Science, Pilani.

Author details: Rohan Badlani is an 2nd year undergraduate student at Birla Institute of technology and Science, Pilani. Contact Number: +91-9660582805; Email address: rohan.badlani@gmail.com..

II. Network Security System

The network security system analyzes the flow the data to the users of a network by the access rights a particular user has been provided with by the organization. These systems first of all identify the type of the user and the rights specified to that particular user. This phenomenon is called authentication. Different levels of authentication may be used by the network security systems. A two way token would mean using a token for the authentication process and is generally used when we want the user to go through the authentication process as soon as possible. A three way authentication involves the use of biometric analysis of the user. This is more secure way to identify the user over the network. Now, when the network security system identifies the user and hence its type, immediately the firewall imposes all the access rights to the user and these rights govern the kind of activity that the user can do. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted. However, worms might come in the way of the normal operation of the network security systems and may cause sensitive flow of data also. Some example of the network security systems are – Intrusion Detection System, Intrusion Prevention System, Anomaly based Intrusion detection system, APIDS – Application protocol based intrusion detection system, etc. Certain surveillance systems may also be incorporated to detect early attacks in the system. One of the most important requirements of such a system is that the communication between the systems should be highly encrypted and should not be such that a programmed computer is able to identify the encryption key for the network security systems.

III. Requirements of a Network Security System

First and foremost requirement of the network security system is the firewall and proxy restrictions to keep the unwanted people out of the network and allow only limited access to certain users based on their authentication. Authentication is the second requirements – The network security systems require strong password combinations that need to be frequently changed so that the intruder is not able to guess the pattern of the passwords. Moreover, an even more robust password combination is required in the case of Wireless networks. The communication between the network security systems should be highly encrypted.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Physical security precautions should be taken if business is large and prone to intrusions. Relatively high vigilance should be imposed on the entry areas and the user should be asked to enter the password combination whenever he tries to access a higher scale of sensitive information. All network hardware should be placed in a secure zone and all the hosts should be in a private network. All servers must be in a DMZ or firewall from inside or outside. Also security fencing is needed by the network security systems to mark the boundaries of the setup.

IV. PROTOCOLS

Dial-up connections generally used modems called Unix to Unix copy for connecting to unix hosts. This UUCP has limited security and is difficult to trick into. In order to improve the security, another layer of authentication can be added called Sequence Number which is a sequence of numbers generated when a connection is set up between two unix hosts. A few while later this UUCP was integrated into the internet with an easy addressing mechanism.

Then came in the Internet – the network of networks which is based on a set of rules governed by Transmission Control Protocol and the Internet Protocol. The TCP is responsible for providing reliable, ordered, error-checked delivery of data between computer systems connected over a Local Area Network or intranet. The Internet Protocol relays datagrams across network boundaries. Thus for establishing the connection among different hosts it is mandatory to be aware of the TCP/IP basic structure. The IP and TCP constitute two important layers of the OSI Model – namely the network and transport layer respectively. Fig 1 shows the OSI Reference model and primarily focuses on the TCP and IP.

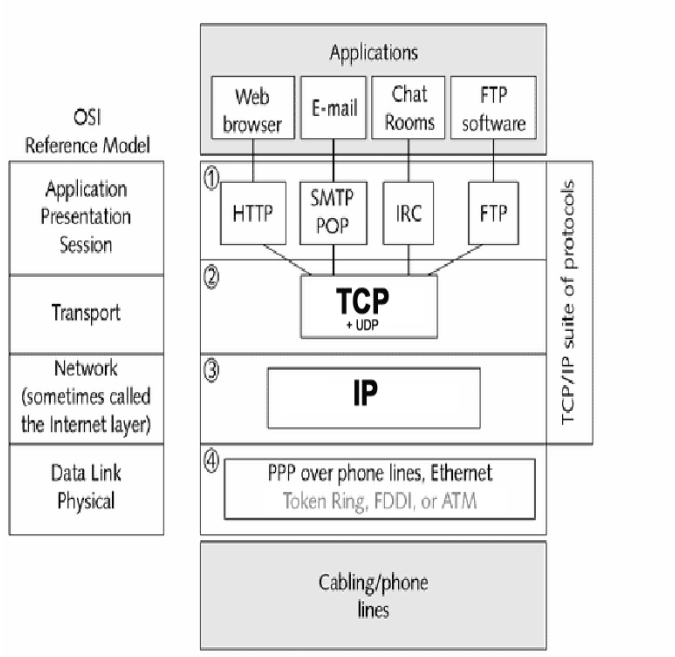

Fig 1: Showing the OSI Model with specific focus on TCP and IP.

It is at the Network Layer where the physical address of the user is mapped with the logical address and also the routing takes place. Thus security aspects of Internet Protocol play a key role in the security over a network. There can variety of attacks against the IP. Some of these are mentioned below.

1) IP Spoofing: IP spoofing is the creation of IP Packets with a forged IP Address or IP address of some other host on the network with the purpose of concealing the identity of the sender. Generally, the routers access control decides what type of packets can pass through it and which cannot pass based on the IP address of the sender. Sometimes, certain applications also allow login based on the IP address of the user

2) IP Session Hacking: Session hacking is the exploitation of a valid computer session or a session key to gain unauthorized access to information or services in a computer system. It is generally used to refer to the theft of a magic cookie (a cookie is used to identify a particular event or transaction) used to authenticate the user to a remote server. Normally this happens in those remote sessions that do not use any encryption.

V. NETWORK THREATS

There is variety of network threats. Some of them have been mentioned below:

1. Unauthorized access: The unauthorized access includes those requests coming from hosts/ users who claim to be someone else over the network either through session hacking or IP Spoofing. This is generally done for execution of illicit commands – attack seeking access to the host intending to change the configuration set of the host as an administrator. This may also be done for access to confidential information and the user may even sometimes alter this confidential information.

2. Denial of Service (DoS): The attacker's program makes a connection on some service port by somehow forging the packet's header information claiming that the packet has been sent from an entirely different location.

The attacker generally gains access to a particular host via internet connection, modem or through physical devices. Firewall is responsible for preventing this kind of attack. There are generally either block traffic or allow the traffic. Following are certain techniques that can be used to avoid attacks on host via network.

A. **Firewall:** There is always a two way traffic flow that exists between the host and the internet. Firewall can be defined as a system that forms by enforcing an access

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

control policy barrier between the two or more networks. Firewalls can be impregnated on both software as well as hardware systems, and a combination of both. Firewalls generally prevent unauthenticated interactive login from the outside world. Sophisticated firewalls prevent the outside world users from accessing sensitive information and at the same time allow the users inside the network to freely access the information over the network.

B. **Bastion Host:** These are Unix OS based hosts that have been customized in order to reduce its functionality to only what is necessary to provide its function. It controls the access between the Internet and the Intranet.

C. **Router:** It is a special purpose switch used to route packets on the networks they connect as per the configuration script running on it so that the packets are routed to the proper direction.

D. **Access Control List:** The Access Control List (ACL) are certain policies employed to limit the sorts of packets that are allowed to pass through the routers. These also include the origination address, destination address and the destination service port.

E. **DMZ (Demilitarized Zone):** The DMZ is a part of the firewall. It is a network that is neither part of the secure network nor a part of insecure network. It is somewhere in the middle – connecting the untrusted to the trusted network. Basically DMZ provides several layers of security to unauthorized access into a private network. An intruder thus has access only to the equipment in the DMZ, rather than any other part of the network. The term is derived from the function of DMZ of not allowing any military action over the trusted inner network.

F. **Proxy:** A proxy server is an intermediate server between the client and the server that actually fetches the requests made by the client and offers services to it. The job of this proxy server is to evaluate the requests made by the clients, process them, and only allow those requests to be passed to the actual servers that are allowed for that particular user. In today's time, most of the proxies are web based proxies that facilitate the access on the World Wide Web. Following are a few benefits of using proxy servers:

1. Keep machine behind the proxy servers to be anonymous.

2. Speed up the resources using caching. Web proxies generally cache web pages from web servers.

3. Preventing downloading of the same resources – files, pages, etc multiple times and hence save bandwidth.

4. To scan the content from server to client for malware before delivery.

5. To bypass website restrictions at work.

6. Access enhancement/restrictions based upon organizational policies.

VI. Types of Firewall

Firewalls can be mainly categorized into three broad categories.

1. Application gateways: It consists of a security that augments a firewall or NAT employed in a computer network. These are made of bastion hosts that run special server to act as a proxy server. Clients generally use gateways to connect to the internet. Scripts are normally written to configure the application gateway. Depending on the script the gateway decides what type of data can flow.

2. Packet Filtering: This technique is used by the firewalls with inclusion of ACLs. If packet filtering is not imposed on the routers, then they allow all the packets to pass through it. Package filtering is advantageous over application gateway as the feature of the access control is performed at a lower OSI layer, generally the transport layer. This makes packet filtering faster than application gateways. The basic idea behind packet filtering is segregating the packets on the basis of their source and destination IP addresses. However, TCP/IP does not always guarantee that the source is what it really claims to be. Thus we require a combination of layers of packet filters to distinguish between a packet belonging to the internet or to an internal network and also to find out the exact source IP address of the source with surety.

3. Combination of Hybrid Systems: The concept of Application gateway is hybridized with the idea of packet filtering. There are certain more check points added that require the authentication of the user. When the connection is successfully established, the session layer comes into picture and the packet filtering ensures that only those packets are passed that are part of the message and are sent from the same IP address. The combination of both the application layer gateway and packet filtering is that it provides services to Internet at the same time maintains the security of the internal network – the intranet as now the intruder needs to break through two routers in order to access the internal network.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

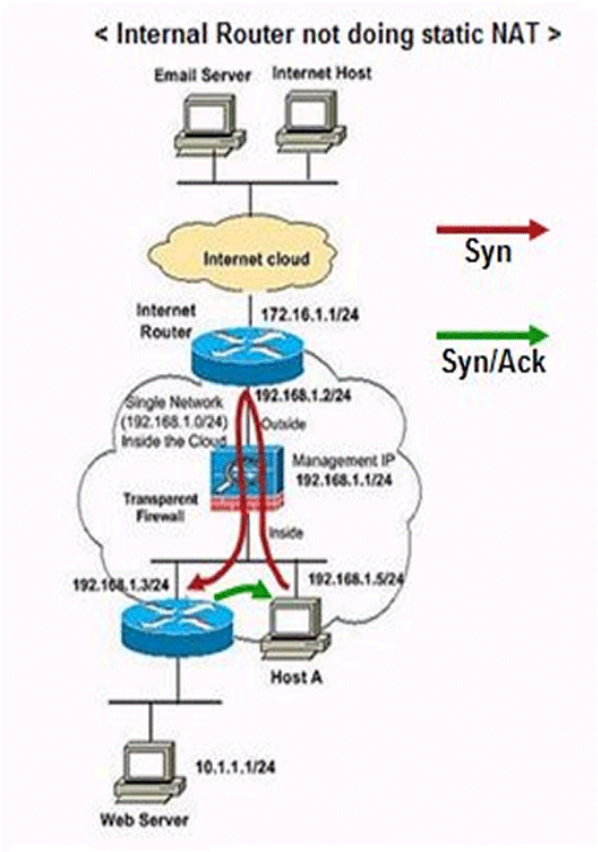

Fig 2: Transparent Firewall

The only entry point to an internal network should be through a firewall. In case of dial-up networks, modems should be the entry point to the network. The architecture of the firewall depends upon the size of the network, the type of devices, bandwidth, etc. Cryptographic techniques should be used between routers to restrict the flow of traffic between them. Virtual Private network technology can also be used to connect different branches of the organization over a private leased line. The sessions currently used by the different branches would go through the link privately as the link has been encrypted, without showing up to the real world.

VII. Development of Security System

The security system is a design issue which requires a lot of research to it. The best combination of technology can be integrated and then deployed for better performance. As an example, the network architect can decide whether to have one or two firewalls, DMZ, Packet filter, Application gateway, etc for all the services. Provision of 2 firewalls will provide more security to the network. The deployed system should have its own defined policies as adopted by the systems administrator. This system should deny unauthorized access to resources to provide close monitoring of the sensitive data

.

VII. Analysis of Different Security Systems

The available security systems should be studied in depth and can be summarized based on their demands and can be summarized on the basis of their merits and demerits. Each system has the following overheads – cost of maintenance, reliability and feasibility. Design of security systems is complicated. Scalability and flexibility of the security systems should be analyzed. The security system can be centralized and it must enforce organization wide security policies. There is no formal way to describe the architectural structure of the security system nor there is any specific properties to be satisfied by them. These techniques are based upon abstract mathematical models. In practice there exists no way to verify and predict the composition of security systems that satisfies the properties. It is highly specific on the network for which the security system has to be developed. However, there can be certain security systems that are simulated for different situations and be utilized in majority of organizations with subtleties in their systems. This type of security systems act as models that can be further customized to cater to the requirements of the network – something like the ERP system, which is most generally customized by the organizations depending upon their own needs.

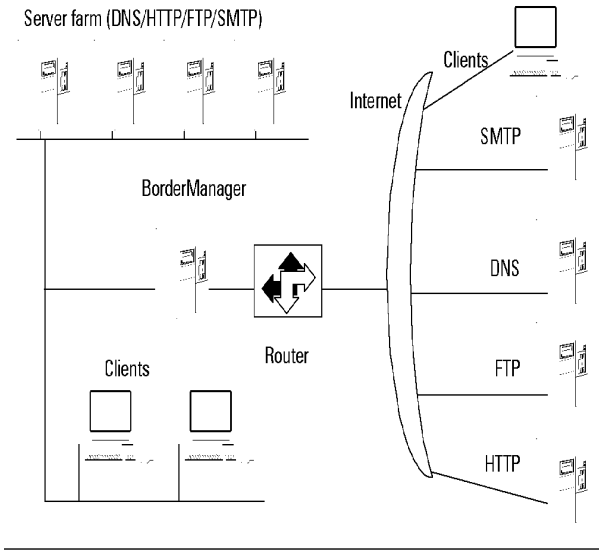

Fig 3: Server Farm

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Country	Cyber Attacks
USA	355,341
Brazil	337,977
Italy	288,607
Israel	143,943
Taiwan	907,102
Argentina	185,720
Australia	255,777
Japan	133,908
Russia	2,402,722
Germany	780,425
Poland	162,235
Hungary	367,966
Romania	350,948
Ukraine	566,531

Fig 4: Table showing approximate cyber attacks originated in various countries. (Feb 2013.)

A. Simulation:

A security system is to be created based on the security model design issues. The design issues at various levels include – (1) Very good architecture of the security model. (2) Specification of system wide security constraints. (3) Decompose the system wide security constraints into intermediate constraints to design the components. (4) Verification of the constraints between system wide and the component wide constraints. (5) Incremental design and verification of components.

B. Existing software for network security:

Some of the freely available softwares are OSSEC (Host based Intrusion Detection System), Snort (Network Intrusion Detection System), Prelude (Hybrid based Intrusion detection system), etc.

C. Testing of Security system:

Once the system design is ready, it must be tested at the component and the system level. This is a stage where a lot of study is required in order to test all the constraints imposed on the system by each of the component or sub-components.

D. *Performance of the security system:* The performance of the designed security system, is to be seen over a period of time under different conditions. It should be carried on some factors – cost, hardware, feasibility and efficiency. The security policies formed in a security system enforces on every component of the system.

VIII. Future Scope

The aim of this entire study is to come up with a network security system that can be used over variety of network architectures and is more scalable and flexible.

IX. Conclusion

Unauthorized access and Denial of service - being two of the most common threats on the Internet and it's growth over the years compels us to find out more secure, efficient and scalable network security systems that forbid the attacker from intruding into secure internal networks for confidential information or other purposes. Firewalls (Application gateway, Packet filters, and a combination of both), proxy servers, Demilitarized Zone (DMZ) and ACL are some of the technology used in today's network security. However these are generally not very highly organized to obtain optimum security requirements. There is some possibility of intrusion through these systems. This calls for the design of newer systems simulated for various situations such that more reliable and secure network security systems can be designed.

Acknowledgment

I am grateful to the management of BITS, Pilani for allowing me to conduct this study on network systems. This work was supported by Computer Science Department, BITS, Pilani and I express my deep gratitude to all the professors for providing their valuable guidance, encouragement, support and advising technical points from time to time in the course of preparation of this review paper.

References

[1] Yi Dung and Jiacun Wang et. al.. An Approach for modeling and Analysis of Security Systems Architechtures, IEEE Transactions on knowledge and Data Engineering, Vol 15, No 5, September 2003.

[2] Matt Curtin Introduction to Network, March 1997.

[3] Forouzan, Behrouz A & S. C. Fegan. Data Communication and Networks, 2006

[4] Kurose, James F & KW Ross, Computer Networking, Pearson Education,2010.

[5] D Shukla, K Verma, J Dubey, Cyber Crime based Curve Fitting in internet Traffic Sharing in Computer Network, 2012

[6] Andrew K. Adams and Adam J. Lee, "Combining Social Authentication and Untrusted Clouds for Private Location Sharing", in Proceedings of the 18th ACM Symposium on Access Control Models and Technologies (SACMAT), June 2013.

[7] M. Mathis, J. Heffner, R. Reddy, "Web100: Extended TCP Instrumentation for Research, Education and Diagnosis," *ACM Computer Communications Review*, Vol **33**, (3), July 2003
.

[8] V. Paxson, J. Mahdavi, A. Adams, M. Mathis, "An Architecture for Large-Scale Internet Measurement", *IEEE Communications* 36(8), pp 48-54, August 1998.

[9] F. Wimberly, M. Lambert, N. Nystrom, A. Ropelewski, W. Young, "Porting Third-Party Applications Packages to the CRAY T3D: Programming Issues and Scalability Results", Parallel Computing, number 22, pp. 1073-1089, 1996.

[10] J. C. Honig, D. Katz, M. Mathis, Y. Reckhter and J. Y. Yu, "Applications of the Border Gateway Protocol in the Internet", June 1990, RFC1164 USC/Information Sciences Institute.

[11] W.J. Buchanan. *Handbook of Data Communications and Networks.*Kluwer, 1998.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)