© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

CURRENT NETWORK SECURITY: ISSUES AND CHALLENGES

Gourav Rathor , Devank V. Rathore

***Abstract*- Theoretical Secure Network has now turned into a need of any association. The security dangers are expanding step by step and making rapid wired/remote system and web administrations, unreliable and questionable. Presently – a - days efforts to establish safety lives up to expectations all the more essentially towards satisfying the forefront requests of today's developing commercial ventures. The need is additionally incited into the regions like safeguard, where secure and verified access of assets are the key issues identified with data security. In this paper Author has portrayed the paramount measures and parameters in regards to vast industry/hierarchical prerequisites for building a protected system. Wi-Fi systems are extremely normal in giving remote system access to diverse assets and uniting different gadgets remotely. There are need of diverse necessities to handle Wi-Fi dangers and system hacking endeavors. This paper investigates critical efforts to establish safety identified with diverse system situations, so that a completely secured system environment could be made in an association. Creator likewise has talked about a careful investigation to delineate the negligible set of measures needed for building system security in any association.**

I. INTRODUCTION

System security can be characterized as insurance of systems and their administrations from unapproved change, decimation, or exposure, and procurement of certification that the system performs in basic circumstances and have no hurtful impacts for not client or for representative [6]. It likewise incorporates procurements made in an underlying machine system base, strategies embraced by the system overseer to ensure the system and the system available assets from unapproved access. System security outline requirements can be compressed under the accompanying,

A. Security Attacks

Security attacks can be classified under the following categories:

Passive Attacks

This type of attacks includes attempts to break the system by using observed data. One of the example of the passive attack [8,11] is plain text attacks, where both plain text and cipher text are already known to the attacker. The attributes of passive attacks are as follows:

- Interception: attacks confidentiality such as eavesdropping, “man-in-the-middle” attacks.
- Traffic Analysis: attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation.

Active Attacks

This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one or both directions. [8, 11] The attributes of active attacks are as follows,

- Interruption: attacks availability such as denial-of-service attacks.
- Modification: attacks integrity.
- Fabrication: attacks authenticity.

B. Network Security Measures:

Following measures are to be taken to secure the network [6]:

- A strong firewall and proxy to be used to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package should be installed.

- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.

- When using a wireless connection, use a robust password.

- Employees should be cautious about physical security.

- Prepare a network analyzer or network monitor and use it when needed.

- Implementation of physical security measures like closed circuit television for entry areas and restricted zones.

- Security barriers to restrict the organization's perimeter.

- Fire asphyxiators can be used for fire-sensitive areas like server rooms and security rooms.

C.* Network Security Tools*:

Following tools are used to secure the network :

- N-map Security Scanner is a free and open source utility for network exploration or security auditing.

- Nessus is the best free network vulnerability scanner available.

- Wire shark or Ethereal is an open source network protocol analyzer for UNIX and Windows.

- Snort is light-weight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.
- Net Cat is a simple utility that reads and writes data across TCP or UDP network connections.

Kismet is a powerful wireless sniffer.

II. FOUNDATION

Marin [7] characterized the center down to earth organizing parts of security including machine interruption location, activity dissection, and system checking parts of system security. Flauzac [5] has displayed another methodology for the usage of dispersed security arrangement in a controlled community oriented way, called framework of security, in which group of gadgets guarantees that a gadget is reliable and correspondences between gadgets can be performed under control of the framework approaches. Wu Kehe [13] has characterized data security in three sections - information security, system framework security and system business security, and the system business security model. A hypothetical premise for security barrier for big business programmed generation framework has likewise been created. A Public Key Infrastructure (PKI)-based security schema for remote system has been characterized by Wuzheng [14]. In this [1, 3, 4, 9- 12] different apparatuses and treatment identified with cryptography and system security has been characterized. The most recent issues identified with system security innovation and their pragmatic applications like Advance Encryption Standard (AES), CMAC mode for confirmation and the CCM mode for verified encryption guidelines are additionally examined in an exceptionally elaborative manner. Moreover, different hacking endeavors and their identification, medicinal are likewise examined in an extremely effective manner.

These days, move of data in a more secure and secure path over a system has turned into a significant test for the business. The assaults and the system efforts to establish safety characterize that how utilizing the system security devices, a finer, solid and safe system can be outlined and kept up for an association/industry. This examination concentrates on the issues through which arrange security can be overseen and kept up all the more effectively in an association. Besides the Security routines and a research endeavor will help a ton in understanding the better administration of the system security-controlling in an association.

III. SECURITY METHODS

a. Cryptography

- The most widely used tool for securing information and services [11].

- Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message.

b. Firewalls

A firewall is simply a group of components that collectively form a barrier between two networks.[8,11] There are
three basic types of firewalls.

I) Application Gateways

This is the first firewall and is some times also known as proxy gateways as shown in figure 1. These are made up of bastion hosts so they do act as a proxy server. This software runs at the Application Layer of the ISO/OSI Reference Model. Clients behind the firewall must be categorized & prioritized in order to avail the Internet services. This is been the most secure, because it doesn't allow anything to pass by default, but it also need to have the programs written and turned on in order to start the traffic passing.

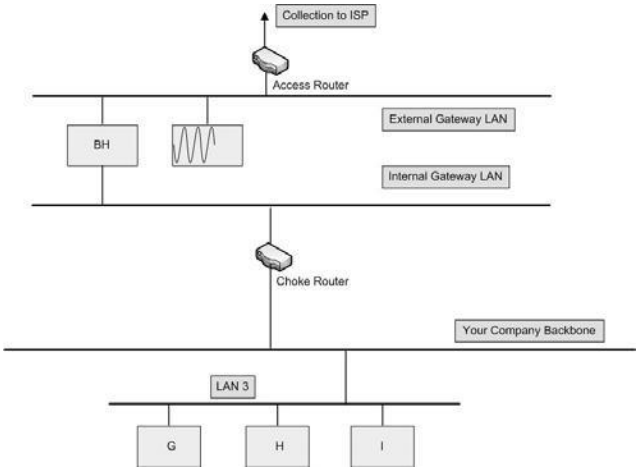

Figure 1: A sample application gateway [8]

II) Packet Filtering

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent through it, without any restrictions as shown in figure 2. ACL's is a method to define what sorts of access is allowed for the outside world to have to access internal network, and vice versa.

This is less complex than an application gateway, because the feature of access control is performed at a lower ISO/OSI layer. Due to low complexity and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. There are problems with this method; thought TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, use layers of packet filters are must in order to localize the traffic.

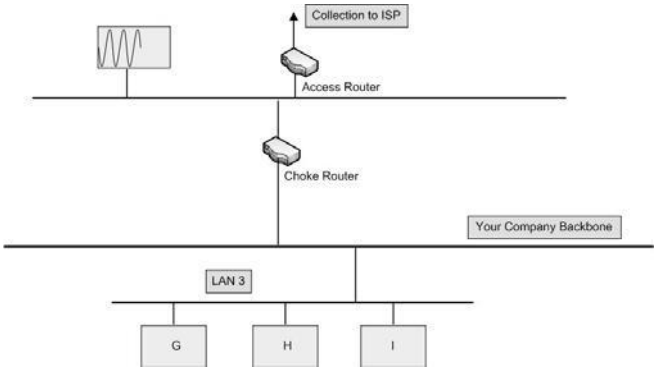

Figure 2: A sample packet filtering gateway [8]

It can differentiate between a packet that came from the Internet and one that came from our internal network. Also It can be identified which network the packet came from with certainty, but it can't get more specific than that.

III) Hybrid Systems

In an attempt to combine the security feature of the application layer gateways with the flexibility and speed of packet filtering, some developers have created systems that use the principles of both. In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure

that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed.

Uses of packet filtering and application layer proxies are the other possible ways. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

IV. SECURITY MANAGEMENT ISSUES

• Ensuring the security strength of the organization is a big challenge nowadays. Organizations have some pre-defined security policies and procedures but they are not implementing it accordingly. Through the use of technology, we should impose these policies on people and process.
• Building and affirming high-quality resources for deployment and efficient management of network security infrastructure.
• Adopting technologies that are easy and cost effective to deploy and manage day-to–day network security operations and troubleshoots in the long run.
• Ensuring a fully secure networking environment without degradation in the performance of business applications.
• On a day-to-day basis, enterprises face the challenge of having to scale up their infrastructure to a rapidly increasing user group, both from within and outside of the organizations. At the same time, they also have to ensure that performance is not compromised.
• Organizations sometimes have to deal with a number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.
• The implementation and conceptualization of security blueprint is a challenge. Security is a combination of people, processes, and technology; while IT managers are traditionally tuned to address only the technology controls.

Network Security cuts across all functions and hence initiative and understanding at the top level is essential. Security is also crucial at the grassroots level and to ensure this, employee awareness is a big concern. Being update about the various options and the fragmented market is a challenge for all IT managers. In the security space, the operational phase assumes a bigger importance. Compliance also plays an active role in security; hence the business development team, finance, and the CEO's office have to matrix with IT to deliver a blueprint.

V. WHAT AN ORGANIZATION MUST DO?

• Organization should be prepared to cope with the growth of the organization, which in turn would entail new enhancements in the network both in terms of applications and size. They should plan security according to the changing requirements, which may grow to include various factors like remote and third-party access.
• Threats are no longer focused on network layer; application layer is the new playground of hackers. Attack protection solutions must protect network, services and applications; provide secure office connection, secure remote employee access, resilient network availability, and controllable Internet access.
• The ideal solution for internal security challenges is not only a conventional security product but it must contain the threats (like worms), divide the network, protect the desktop, server and the data center.
• About 70 percent of new attacks target Web-enabled applications and their number is growing. Enterprises should, therefore, deploy Web security solutions that provide secure Web access as well as protect Web servers and applications. The security solutions must be easy to deploy, and they should also provide integrated access control.

VI. TECHNOLOGY OPTIONS

Leading security vendors offer end-to-end solutions that claim to take care of all aspects of network security.
End-to-end solutions usually offer a combination of hardware and software platforms including a security management solution that performs multiple functions and takes care of the entire gamut of security on a network. An integrated solution is one that encompasses not only a point-security

problem (like worms/intrusion) but one that also handles a variety of network and application layer security challenges. Available products can be categorized in the following streams,

ASIC based appliances: The move is from software- based security products that run on open platforms to purpose-built, ASIC-based appliances, just like the path the routers have followed in the last decade.

SSL-VPN: Greater awareness of encryption on the wire in the form of SSL and IP-VPNs. People are increasingly aware of the security risks in transmitting data over the wire in clear text. To address this, SSL-VPN has hastened acceptance of VPNs for end users and IT departments alike.

Intrusion Detection Prevention Systems: An IPS combines the best features of firewalls and intrusion detection system to provide a tool that changes the configurations of network access control points according to the rapidly changing threat profile of a network. This introduces the element of intelligence in network security by adapting to new attacks and intrusion attempts. Intrusion prevention has received a lot of interest in the user community.

Most organization evolves in their use of intrusion prevention technology. Some will adopt blocking in weeks and rapidly expand their blocking as they see the benefits of accurate attack blocking. Others will start slowly and expand slowly. The key is to reliably detect and stop both known and unknown attacks real time.

VII. WAN SECURITY

In organizations where there are satellite offices in various regions the task of securing the network system is even tremendous. May the organization need to employ something like an Up logic network security system to better automate management of this scattered computers. It's really a challenge to work with networks that span various locations. Just imagine that one will need to fly to that place if the support if not done remotely.

VIII. CASE STUDY

Author has given a case study of a software development company to explore the security mechanisms and the security measures used in the company to establish a secure network environment.

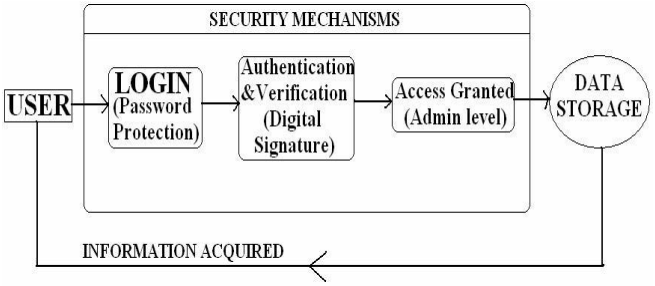

Figure 3: Information flow between user and Data Storage

Figure 3 shows the company's data access and user-database interaction model. Here firstly the originality, authenticity etc is checked and then the user is granted the access for gathering information from data storage at the administrator level. The above diagram is a very small representation of the security mechanisms applied in the company. The company uses its intranet, hubs, routers, data storage units etc, which are managed and arranged by the different professionals at their level.

The information provided to the outsider of the company is always general and the important data and information are not even leaked or opened in front of the employees. Only the particular data management section handles the security of data and tries to maintain the importance of the data. Figure 4 represents the dataflow in the company and showing the mechanism that how DBA can use and arrange data better than a user and why he is more powerful? This diagram shows that how a user/employee in a company goes through the data access in a
company. It can vary by the no. of users, employees.

For this company, the user first goes through a secured firewall for acquiring the information but he can only read the gathered information and can only transfer it to the third party as to second user with no modification and alteration whereas administrator can go through all the read and write operations in the database, he can check the authenticity, originality of the original message time to time and can maintain the security level by this mean. The encrypted information provided by the Database to user 1 is just for his reading works only, he neither can use, modify nor can alter this information.

The company chosen by the author doesn't have any branches at all. The company follows a security hierarchy, which is applicable to all employees while assessing any resources on the network.

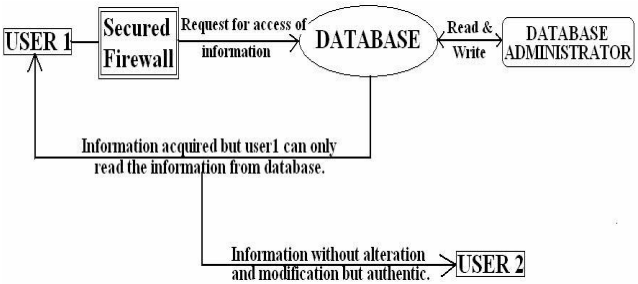

Figure 4: Interaction between users

For maintaining the level of security, there are many professionals' related to ethical hacking, information security and network security and due to the field of crackers growing day by day network level security and information security have become a need of every company whether it is big or small!

IX. FUTURE WORK

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work. Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible.

Generally the network security system tools in the past were command line interface (CLI) based. It's only in this last few years that more and more computer and network administration task is done remotely through a web-based tool. Network system tools are very important no matter whether they are GUI or CUI, in today's heavily inter-connected era.

X. CONCLUSION

Security has become important issue for large computing organizations [6]. There are different definitions and ideas for the security and risk measures from the perspective of different persons. The security measures should be designed and provided, first a company should know its need of security on the different levels of the organization and then it should be implemented for different levels. Security policies should be designed first before its implementation in such a way, so that future alteration and adoption can be acceptable and easily manageable. The security system must be tight but must be flexible for the end-user to make him comfortable, he should not feel that security system is moving around him. Users who find security policies and systems too restrictive will find ways around them.

Author have shown the minimum set of requirements parameters to establish a secure network environment for any organization with the help of case study of a software development firm. Security policies should not be fixed rather than it should be flexible enough to fulfill the need of an organization as well as it should be capable enough to tackle future security threats while at the same time easily manageable and adoptable.

REFERENCES

[1] A beginner's guide to network security, CISCO Systems, found at http://www.cisco.com/warp/public/cc/so/neso/sqso/ beggu_pl.pdf, 2001

[2] Al-Akhras, M.A., "Wireless Network Security Implementation in Universities" In Proc. of Information and Communication Technologies, 2006. ICTTA '06., Vol. 2, pp. 3192 – 3197, 2006.

[3] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley

[4] Farrow, R., Network Security Tools, found at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf

[5] Flauzac, O.; Nolot, F.; Rabat, C.; Steffenel, L.-A., "Grid of Security: A New Approach of the Network Security", In Proc. of Int. Conf. on Network and System Security, 2009. NSS '09, pp. 67-72, 2009.

[6] Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-network-security-system.htm

[7] Network Security Assessment, 2nd Edition