MODERN NETWORK SECURITY: ISSUES AND CHALLENGES

J Bramaramba[1], B Eswar Babu[2], T Devi[3]

[1]*Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad*

[2]*Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad*

[3]*Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad*

Abstract — Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. Now – a - days security measures works more importantly towards fulfilling the cutting edge demands of today's growing industries. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. In this paper Author has described the important measures and parameters regarding large industry/organizational requirements for establishing a secure network. Wi-Fi networks are very common in providing wireless network access to different resources and connecting various devices wirelessly. There are need of different requirements to handle Wi-Fi threats and network hacking attempts. This paper explores important security measures related to different network scenarios, so that a fully secured network environment could be established in an organization. Author also has discussed a case study to illustrate the minimal set of measures required for establishing network security in any organization.

Keywords — Cryptography; Security Attacks; Security Measures; Security Tools; WAN; Security Factors; Firewalls; Gateways; Intrusion Detection.

1. INTRODUCTION

  Network security can be defined as protection of networks and their services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no harmful effects for neither user nor for employee [6]. It also includes provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access. Network security design constraints can be summarized under the following,

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 [4]:
- 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.

2. BACKGROUND

Marin [7] defined the core practical networking aspects of security including computer intrusion detection, traffic analysis, and network monitoring aspects of network security. Flauzac [5] has presented a new approach for the implementation of distributed security solution in a controlled collaborative manner, called grid of security, in which community of devices ensures that a device is trustworthy and communications between devices can be performed under control of the system policies. Wu Kehe [13] has defined information security in three parts - data security, network system security and network business security, and the network business security model. A theoretical basis for security defense for enterprise automatic production system has also been established. A Public Key Infrastructure (PKI)-based security framework for wireless network has been defined by Wuzheng [14]. In this [1, 3, 4, 9-12] various tools and treatment related to cryptography and network security has been defined. The latest issues related to network security technology and their practical applications like Advance Encryption Standard (AES), CMAC mode for authentication and the CCM mode for authenticated encryption standards are also discussed in a very elaborative way. In addition, various hacking attempts and their detection, remedial are also discussed in a very efficient way.

Nowadays, transfer of information in a safer and secure way over a network has become a major challenge for the industry. The attacks and the network security measures define that how using the network security tools, a better, healthy and safe network can be designed and maintained for an organization/industry. This research focuses on the issues through which network security can be managed and maintained more efficiently in an organization. Furthermore the Security methods and a case study will help a lot in understanding the better management of the network-security-controlling in an organization.

3. 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.
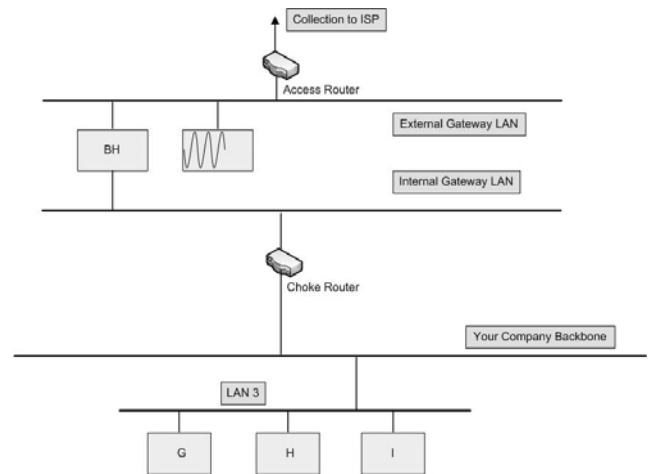

Figure 1: A sample application gateway [8]

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.
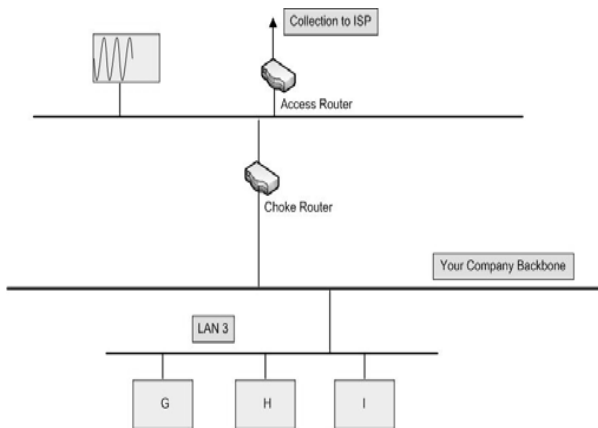
Figure 2: A sample packet filtering gateway [8]

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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.
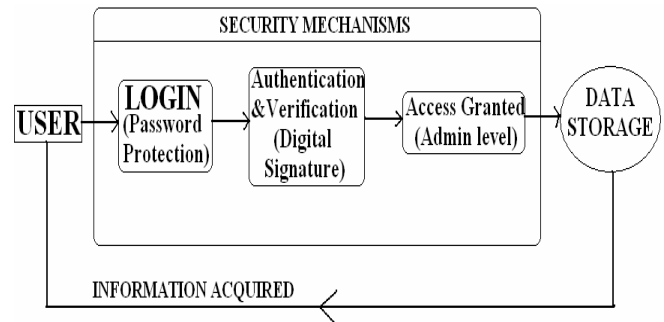

Figure 3: Information flow between user and Data Storage

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.
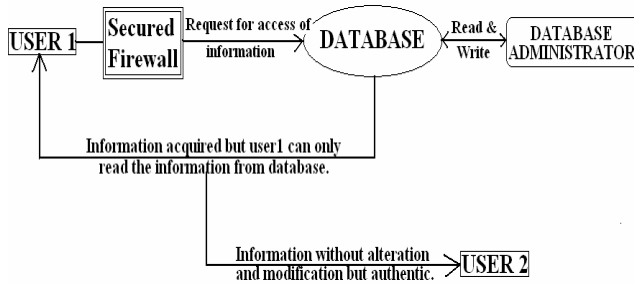

Figure 4: Interaction between users

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!

9. 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.

10. 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.

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] Marin, G.A. (2005), "Network security basics", In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.

[8] Matt Curtin, Introduction to Network security, found at http://www.cs.cornell.edu/Courses/cs519/2003sp/slides/15_securitybasics.pdf, March 1997.

[9] McClure, S., Scambray J., Kurtz, G. (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, TMH.

[10] Murray, P., Network Security, found at http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout.pdf

[11] Stallings, W. (2006): Cryptography and Network Security, Fourth Edition, Prentice Hall.

[12] Stallings, W. (2007): Network security essentials: applications and standards, Third Edition, Prentice Hall.

[13] Wu Kehe; Zhang Tong; Li Wei; Ma Gang, "Security Model Based on Network Business Security", In Proc. of Int. Conf. on Computer Technology and Development, 2009. ICCTD '09, Vol. 1, pp. 577-580, 2019

[14] Wuzheng Tan; Maojiang Yang; Feng Ye; Wei Ren, A security framework for wireless network based on public key infrastructure, In Proc. of Computing, Communication, Control, and Management, 2019. CCCM 2019, Vol. 2, pp. 567 – 570, 2019