Network Security: A Comprehensive Survey of Challenges and Emerging Issues

Dr. K. Venkatesan, Dr. Sneha R. Patel, Dr. Abhinav Kumar
Department of Mathematics, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India;
Department of Mathematics, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India;
Department of Applied Mathematics, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India

ABSTRACT

Secure Network has currently become a necessity of any organization. The safety threats are increasing day by day and creating high speed wired/wireless network and net services, insecure and unreliable. currently – a - days security measures works additional significantly towards fulfilling the innovative demands of today's growing industries. the requirement is additionally elicited in to the areas like defense, wherever secure and attested access of resources are the key problems associated with info security.This paper has delineate the necessary measures and parameters relating to giant industry/organizational necessities for establishing a secure network. Wi-Fi networks are quite common in providing wireless network access to completely different resources and connecting varied devices wirelessly. There are would like of various necessities to handle Wi-Fi threats and network hacking tries. This paper explores necessary security measures associated with completely different network eventualities, so a totally secured network setting might be established in a company. Author conjointly has mentioned a case study as an example the marginal set of measures needed for establishing network security in any organization.

Keywords: *Intrusion Detection, Security Attacks, Security Measures, Security Tools, WAN, Security Factors, Firewalls, Gateways.*

I. INTRODUCTION

Network security may be outlined as protection of networks and their services from unauthorized alteration, destruction, or revealing, and provision of assurance that the network performs in important things and haven't anyharmful effects for neither user nor for worker [6]. It conjointly includes provisions created in associate degreeunderlying network infrastructure, policies adopted by the network administrator to safeguard the network and also the network-accessible resources from unauthorized access. Network security style constraints may be summarized below the subsequent,

A. Security Attacks

Security attacks can be classified under the following categories:

Passive Attacks

This type of attacks includes makes an attempt to interrupt the system by mistreatment discovered knowledge. one in all the instance of the passive attack [8,11] is apparent text attacks, wherever each plain text and cipher text are already proverbial to the aggressor. The attributes of passive attacks are as follows:

• Interception: attacks confidentiality like eavesdropping, "man-in-the-middle" attacks.

• Traffic Analysis: attacks confidentiality, or obscurity. It will embrace trace back on a network, cathode-ray tuberadiation.

Active Attacks

This type of attack needs the aggressor to send knowledge to 1 or each of the parties, or block the information stream in one or each directions. [8, 11] The attributes of active attacks are as follows,

• Interruption: attacks convenience like denial-of-service attacks.

• Modification: attacks integrity.

• Fabrication: attacks credibility.

B. **Network Security Measures:**

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

• a robust firewall and proxy to be wont to keep unwanted individuals out.

• a robust Antivirus computer code package and web Security computer code package ought to be put in.

• For authentication, use sturdy passwords and alter it on a weekly/bi-weekly basis.

• once employing a wireless affiliation, use a sturdy watchword.

• workers ought to take care concerning physical security.

• Prepare a network analyser or network monitor and use it once required.

• Implementation of physical security measures like circuit tv for entry areas and restricted zones.

• Security barriers to limit the organization's perimeter.

• hearth asphyxiators is used for fire-sensitive areas like server rooms and security rooms.

C. Network Security Tools:

Following tools are wont to secure the network [4]:

• N-map Security Scanner could be a free and open supply utility for network exploration or security auditing.

• Nessus is that the best free network vulnerability scanner on the market.

• Wire shark or Ethereal is associate open supply network protocol analyser for UNIX and Windows.

• Snort is light-weight network intrusion detection and interference system excels at traffic analysis and packet work on scientific discipline networks.

• internet Cat could be a easy utility that reads and writes knowledge across transmission control protocol or UDP network connections.

• kismat could be a powerful wireless someone.

II. BACKGROUND

Marin [7] outlined the core sensible networking aspects of security together with laptop intrusion detection, traffic analysis, and network watching aspects of network security. Flauzac [5] has given a brand new approach for the implementation of distributed security answer in a very controlled cooperative manner, known as grid of security, during which community of devices ensures that a tool is trustworthy and communications between devices is performed in check of the system policies. Shanghai dialect Kehe [13] has outlined data security in 3 elements - knowledge security, network system security and network business security, and therefore the network business security model. A theoretical basis for security defense for enterprise automatic production system has conjointly been established. A Public Key Infrastructure (PKI)-based security framework for wireless network has been outlined by Wuzheng [14]. In this [1, 3, 4, 9- 12] numerous tools and treatment associated with cryptography and network security has been outlined. the most recent problems associated with network security technology and their sensible applications like Advance cryptographycustomary (AES), CMAC mode for authentication and therefore the

CCM mode for attested cryptography standards arementioned during a} very elaborative approach. additionally, numerous hacking makes an attempt and their detection, remedial are mentioned during a} very economical approach.

Nowadays, transfer of data in a very safer and secure over a network has become a serious challenge for the trade. The attacks and therefore the network security measures outline that however mistreatment the network security tools, a better, healthy associated safe network is designed and maintained for an organization/industry. This analysis focuses on the problems through that network security is managed and maintained a lot of with efficiency in a company. moreover the protection strategies and a case study can facilitate a great deal in understanding the highermanagement of the network-security-controlling in a company.

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 primary firewall and is a few times additionally called proxy gateways as shown in figure one. These are created of bastion hosts so that they do act as a proxy server. This software package runs at the applying Layer of the ISO/OSI Reference Model. purchasers behind the firewall should be classified & prioritized so as to avail the web services. this is often been the foremost secure, as a result of it doesn't permit something to locomote default, however it additionally have to be compelled to have the programs written and turned on so as to start out the traffic passing.

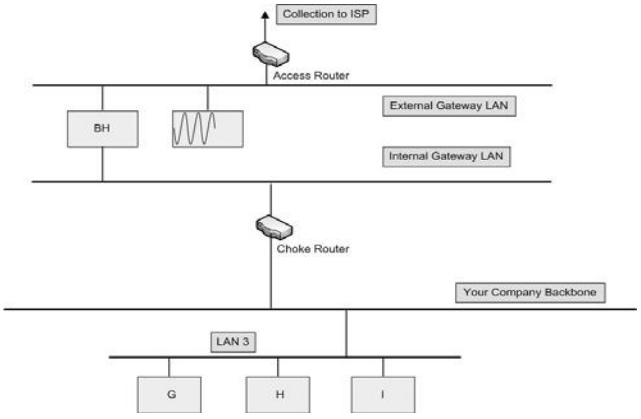

Figure 1: A sample application gateway [8]

II) Packet Filtering

Packet filtering may be a technique whereby routers have ACLs (Access management Lists) turned on. By default, a router can pass all traffic sent through it, with none restrictions as shown in figure a pair of. ACL's may be a

technique to outline what kinds of access is allowed for the skin world to own to access internal network, and contrariwise.

This is less advanced than Associate in Nursing application entree, as a result of the feature of access management is performed at a lower ISO/OSI layer. thanks to low quality and also the incontrovertible fact that packet filtering is completed with routers, that are specialised computers optimized for tasks associated with networking, a packet filtering entree is usually a lot of quicker than its application layer cousins. engaging at a lower level, supporting new applications either comes mechanically, or may be a straightforward matter of permitting a selected packet kind to meet up with the entree. There are issues with this method; thought TCP/IP has absolutely no means that of guaranteeing that the supply address is basically what it claims to be. As a result, use layers of packet filters are should so as to localize the traffic.

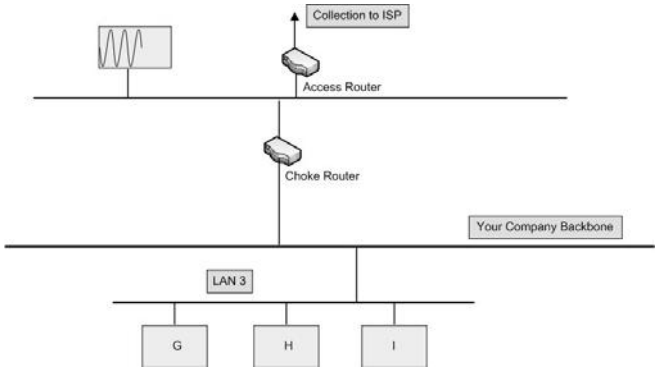

Figure 2: A sample packet filtering gateway [8]

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 a shot to mix the protection feature of the applying layer gateways with the pliability and speed of packet filtering, some developers have created systems that use the principles of each. In a number of these systems, new connections should be genuine and approved at the applying layer. Once this has been done, the rest of the association is passed right down to the session layer, wherever packet filters watch the association to confirm that solely packets that are a part of AN current (already genuine and approved) voice communication are being passed.

Uses of packet filtering and application layer proxies are the opposite doable ways in which. the advantages here embody providing a live of protection against your machines that give services to the web (such as a public web server), additionally as give the protection of AN application layer entree to the inner network. in addition, mistreatment this methodology, AN assaulter, so as to urge to services on the inner network, can ought to break through the access router, the bastion host, and also the choke router.

IV. SECURITY MANAGEMENT PROBLEMS

• Guaranteeing the protection strength of the organization may be a massive challenge these days. Organizations have some pre-defined security policies and procedures however they're not implementing it consequently. Through the utilization of technology, we should always impose these policies on individuals and method.

• Building and affirming high-quality resources for readying and economical management of network security infrastructure.

• Adopting technologies that are simple and value effective to deploy and manage day-to–day network security operations and troubleshoots within the end of the day.

• Guaranteeing a totally secure networking atmosphere while not degradation within the performance of business applications.

• On a every day basis, enterprises face the challenge of getting to rescale their infrastructure to a speedily increasing user cluster, each from inside and out of doors of the organizations. At a similar time, they even have to confirm that performance isn't compromised.

• Organizations generally ought to take care of variety of purpose merchandise within the network. Securing all of them whole whereas guaranteeing seamless practicality is one in every of the largest challenges they face while designing and implementing a security blueprint.

• The implementation and conceptualization of security blueprint may be a challenge. Security may be a combination of individuals, processes, and technology; whereas IT managers are historically tuned to handle solely the technology controls.

Network Security cuts across all functions and therefore initiative and understanding at the highest level is crucial. Security is additionally crucial at the grassroots level and to confirm this, worker awareness may be a massive concern. Being update concerning the varied choices and also the fragmented market may be a challenge for all IT managers. within the security area, the operational part assumes an even bigger importance. Compliance conjointly plays a full of life role in security; therefore the business development team, finance, and also the CEO's workplace ought to matrix with IT to deliver a blueprint.

V. WHAT A COMPANY SHOULD DO?

• Organization ought to be ready to deal with the expansion of the organization, that successively would entail new enhancements within the network each in terms of applications and size. they ought to set up security in line with the dynamic needs, which can grow to incorporate varied factors like remote and third-party access.

• Threats are not any longer targeted on network layer; application layer is that the new playground of hackers. Attack shieldion solutions should protect network, services and applications; give secure workplace association, secure remote worker access, resilient network handiness, and manageable web access.

• The perfect answer for internal security challenges isn't solely a traditional security product however it should contain the threats (like worms), divide the network, shield the desktop, server and also the knowledge center.

• Concerning seventy p.c of latest attacks target Web-enabled applications and their variety is growing. Enterprises ought to, therefore, deploy net security solutions that give secure net access additionally as shield net servers and applications. the protection solutions should be simple to deploy, and that they ought to conjointly give integrated access management.

VI. TECHNOLOGY CHOICES

Leading security vendors provide end-to-end solutions that claim to require care of all aspects of network security.

End-to-end answers typically provide a mix of hardware and software package platforms together with a security management solution that performs multiple functions and takes care of the whole gamut of security on a network. AN integrated answer is one that encompasses not solely a point-security drawback (like worms/intrusion) however one that conjointly handles a range of network and application layer security challenges. on the market merchandise is categorised within the following streams,

ASIC based mostly appliances: The move is from software- based security merchandise that run on open platforms to purposeful, ASIC-based appliances, similar to the trail the routers have followed within the last decade.

SSL-VPN: larger awareness of encoding on the wire within the style of SSL and IP-VPNs. individuals are more and more conscious of the protection risks in sending knowledge over the wire in clear text. to handle this, SSL-VPN has hastened acceptance of VPNs for finish users and IT departments alike.

Intrusion Detection hindrance Systems: AN IPS combines the most effective options of firewalls and intrusion detection system to produce a tool that changes the configurations of network access management points in line with the speedily dynamic threat profile of a network. This introduces the component of intelligence in network security by adapting to new attacks and intrusion tries. Intrusion hindrance has received plenty of interest within the user community.

Most organization evolves in their use of intrusion hindrance technology. Some can adopt block in weeks and speedily expand their blocking as they see the advantages of correct attack blocking. Others can begin slowly and expand slowly. The secret is to dependably discover and stop each celebrated and unknown attacks real time.

VII. WAN SECURITY

In organizations wherever there are satellite offices in varied regions the task of securing the network system is even tremendous. might the organization have to be compelled to use one thing like AN Up logic network security system to raised automatize management of this scattered computers. It's extremely a challenge to figure with networks that span varied locations. simply imagine that one can have to be compelled to fly thereto place if the support if not done remotely.

VIII. CASE STUDY

Author has given a case study of a software package development company to explore the protection mechanisms and also the security measures utilized in the corporate to determine a secure network atmosphere.

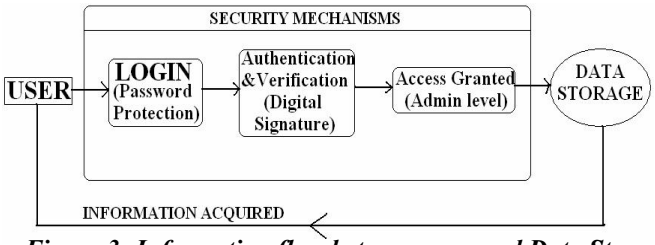

Figure 3: Information flow between user and Data Storage

Figure three shows the company's information access and user-database interaction model. Here first of all the originality, credibleness etc is checked and so the user is granted the access for gathering info from information storage at the administrator level. The higher than diagram may be a terribly tiny illustration of the safety mechanisms applied within the company. the corporate uses its computer network, hubs, routers, information storage units etc, that are managed and organized by the various professionals at their level.

The information provided to the outsider of the corporate is usually general and also the necessary information and data aren't even leaked or opened before of the workers. solely the actual data management section handles the safety of information and tries to keep up the importance of the information. Figure four represents the informationflow within the company and showing the mechanism that however DBA will use and prepare data higher than a user and why he's a lot of powerful? This diagram shows that how a user/employee in an exceedingly company goes through the data access in a

company. It will vary by the no. of users, employees. For this company, the user 1st goes through a secured firewall for effort the data however he can solely scan the gathered information and might only transfer it to the third party on second hand with no modification and alteration whereas administrator can undergo all the read and write

operations within the information, he will check the credibleness, originality of the first message time to time and might maintain the safety level by this mean. The encrypted info provided by the information to user one is simply for his reading works solely, he neither will use, modify nor will alter this info.

The company chosen by the author doesn't have any branches in the least. the corporate follows a security hierarchy, that is applicable to all or any workers whereas assessing any resources on the network.

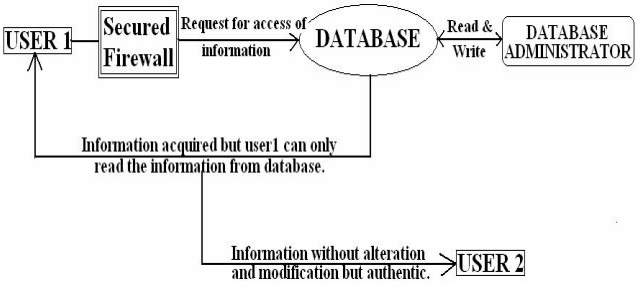

Figure 4: Interaction between users

For maintaining the extent of security, there square measure several professionals' associated with moral hacking, data security and network security and because of the sector of insane growing day by day network level security and knowledge security became a desire of each company whether or not it's huge or small!

IX. FUTURE WORK

Malicious code and different attacks square measure increasing in intensity and also the harm that they cause. With very little time to react, organizations got to become a lot of proactive in their security stance. Reactive security can now not work. Therefore, organizations have to be compelled to higher perceive what the long run trends, risks, and threats square measure in order that they'll be higher ready to form their organizations as secure as potential.

Generally the network security system tools within the past were command interface (CLI) based mostly. It's solely during this previous couple of years that a lot of and a lot of pc and network administration task is completed remotely through a web-based tool. Network system tools square measure important despite whether or not they square measure user interface or CUI, in today's heavily inter-connected era.

X. CONCLUSION

Security has become necessary issue for giant computing organizations [6]. There square measure totally different definitions and ideas for the protection and risk measures from the attitude of various persons. the protection measures ought to be designed and provided, 1st a corporation ought to understand its want of security on the various levels of the organization and so it ought to be enforced for various levels. Security policies ought to be designed 1st before its implementation in such the simplest way, in order that future alteration and adoption may be acceptable and simply manageable. the protection system should be tight however should be versatile for the end-user to form him snug, he mustn't feel that security system is on the road him. Users WHO notice security policies and systems too restrictive can notice ways that around them.

Author have shown the minimum set of necessities parameters to determine a secure network surroundings for any organization with the assistance of case study of a software system development firm. Security policies mustn't be mounted instead of it ought to be versatile enough to meet the requirement of a company similarly because it ought to be capable enough to tackle future security threats whereas at an equivalent time simply 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.html*

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, 2009*

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, 2009. CCCM 2009, Vol. 2, pp. 567 – 570, 2009*