

Network Security

Punam Dhage, Parth Lashkare, Nikita Narole

Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

Article Info

Volume 8, Issue 1

Page Number: 344-350

Publication Issue :

January-February-2022

Article History

Accepted :20 Feb 2022

Published: 28 Feb 2022

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

I. 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.
- Fabrication: attacks authenticity
- Modification: attacks integrity.

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.
- 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.
- 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.

- 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. 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.

III. SECURITY METHODS

a. Cryptography

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

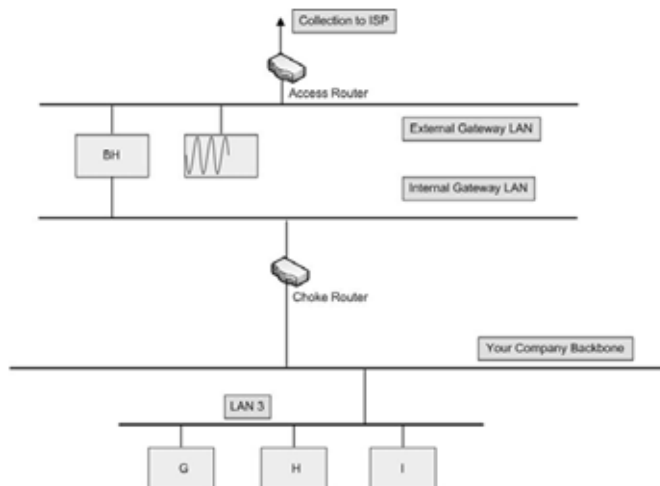
Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message .

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.

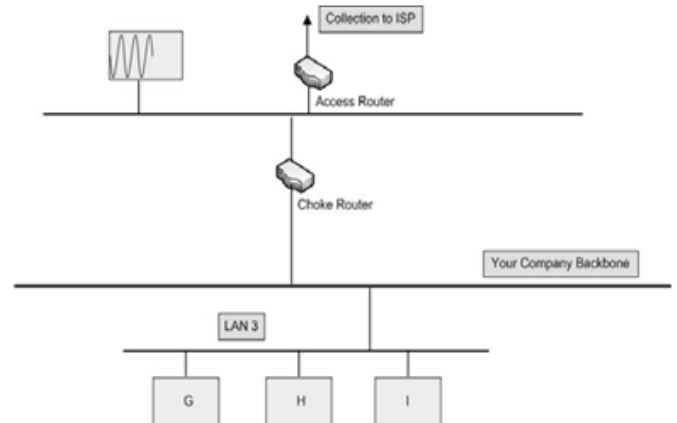


II) Packet Filtering

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; though 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.



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.
- 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. CONS AND PROS

Cons-

Strengthen business connections: Networking is an essential business skill. Identifying opportunities, creating stronger connections and learning valuable information can be critical steps to creating success.

Generate new ideas: Networking is an excellent opportunity for business owners to generate new ideas. By meeting new people, they have the perfect chance to be exposed to fresh information and interesting perspectives.

Enhance visibility: Networking can help individuals to increase their visibility both professionally and personally.

Advancing career: Networking can help many different professionals, not just CEOs.

Pros-

Networking takes time: There are several disadvantages of networking. One of these is the time it takes away from family, hobbies, and your personal life.

May be ineffective: Networking doesn't always lead to a job position or a business opportunity.

May lead to false security: One of the disadvantages of networking is when people think that their network will help them in tough situations.

Networking changes over time: Networking is a valuable tool to use with anyone you meet.

Most people do not know how to network: Networking is a strategy that many people have trouble with.

VI. LITERATURE SURVEY

After discussing about the IEEE 802.1x Introduction, its working and architecture in this section we are briefing about Literature Survey on the various solutions proposed by Researchers / Authors, and which problems still exists. Mentioned implementation of different type of EAP (Extensible

authentication Protocol) techniques. Implementing these techniques is quite complex but in this paper it is shown that by the help of WIRE 1x we can do easily.

It is an OPEN SOURCE implementation of client side because if client side is strong then communication is more secure.

These WIRE 1x easily work with windows and it supports nearly all of the Authentication mechanisms defined in EAP.

WIRE 1x also provide secure manner of communication for user who is using WLAN. It is release in worldwide on 18 Th June 2003.

And from that date large no. of people visited and downloads the source code for different EAP techniques. This paper define all components of WIRE 1x.

It also defines some of EAP techniques like EAP-MD5 EAP- TLS EAP- TTLS EAP- PEAP and also a comparison table has been derived.

It also tell about different open source libraries like.

It has done study of EAP-TLS to compare two type of Extensible Authentication Protocol – transport layer security (EAP-TLS) so that another technique can be provided by using crypto-graphic methods.

The new technique used Elliptical Curve Digital Signature Algorithm (ECDSA) and SHA-256 to provide very high security and also high performance. It also compare it with the existing EAP-TLS method and show that the new techniques provides strong security, high speed and more efficiency by using same level of memory as compare to EAP-TLS. New methods provide a balance between security and optimized uses of resources and time. important concept of WLAN i.e. authentication.

EAP consist of different type of methods for authentication. But shared key and Certificate based methods provide more security to user. This paper mainly concentrate on EAP-FAST because others methods like TLS uses shared secret keys other than certificate due to which performance of EAP-FAST (Flexible Authentication via Secure Tunneling) is

greater the other EAP technique. In this other EAP technique like EAP-TLS, EAP-PEAP, EAP-TTLS are also study.

VII. 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.

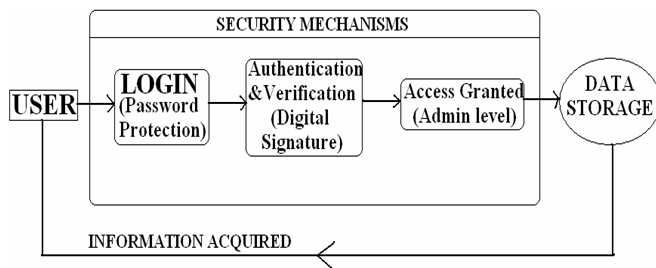
SSL-VPN: Greater awareness of encryption on the wire in the form of SSL and IP-VPNs. People are increasingly aware of the security risks in transmitting data over the wire in clear text. To address this, SSL-VPN has hastened acceptance of VPNs for end users and IT departments alike.

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.

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.



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.

XI. REFERENCES

- [1]. A beginner's guide to network security, CISCO Systems, found at <http://www.cisco.com/warp/public/cc/so/neso/sqs/ob/eggpl.pdf>,
- [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.; Steffene, 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]. Advantages And Disadvantages of Network | Pros and Cons of Network, Difference Between Advantages and Disadvantages - A Plus Topper