"CONSTRUCT NETWORK SECURITY MODEL USING CRYPTOGRAPHY, FIREWALL FOR SOCIAL ORGANIZATION"

Dr.P.Avinash*

Y.Gyana Deepa*

Abstract

In these days, network security plays a very important role in growing networks. As crackers & hackers effect the networks. The network security is prime concept for any big organization such as business, academic or any governmental offices .It requires need to balance the security setup against the risk that are migrated. Various software programs are developed on security basis which has capability of detecting and preventing the attacks from unauthorized side. The most important thing about network security is confidentiality, integrity and availability. This paper discusses various concepts of network security. The various concepts discussed in this paper are Firewall, Cryptography, & Virtual Private Network, need of network security, OSI layer, and advantages of network security architecture.

* Sridevi Women's Engineering College, Telangana.

1. Introduction

Use of the computer and communication using computer, sharing of data is tremendously increases. Network configuration and reconfiguration is easier, faster, and less expensive. However the overall security objectives are preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

Most of the employee work from their home, they share information with their co-worker. Some information is confidential so that both the employee who share the information need strong security. The number of intrusions into computer systems is growing and raising concerns about computer security. Every organization has to define a security policy to display the level of protection which they need to avoid unauthorized access to the resources of their internal network, and to defend against the unauthorized export of private information. The points which will discussed in this paper is :-

- What is network security?
- Network Security Architecture.
- Advantages Network Security Architecture.
- Why the network security is important?
- OSI Layer Model.

2. what is mean by network security?

Before starting with network security, we should know the meaning of the term Network Security. It is the combination of network and security. Simply network means connection between two or more computer. Security means only access only to the authorized user who have some rights. Security means the safety of a state or organization. Perhaps the greatest strength of network is that they enable information to be shared, perhaps the greatest weakness of the network is they enable information to be shared. Security is the trick to permit only legitimate user to share.

Network security consists of the 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 and the effectiveness of these measure combined together. Network security starts from authenticating any user. Once

authenticated, firewall enforces to user access any information they want or any services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.

3. Network Security Architecture

Network security architecture is the planning and design of network to reduce the security risks which came from attackers. This security architecture focused on reducing the security risks and policy through the design and configuration of firewall, routers and other component related to the network security.

Network security is important because it is one of the means to enforce the procedures and system developed by the organization to protect the information.

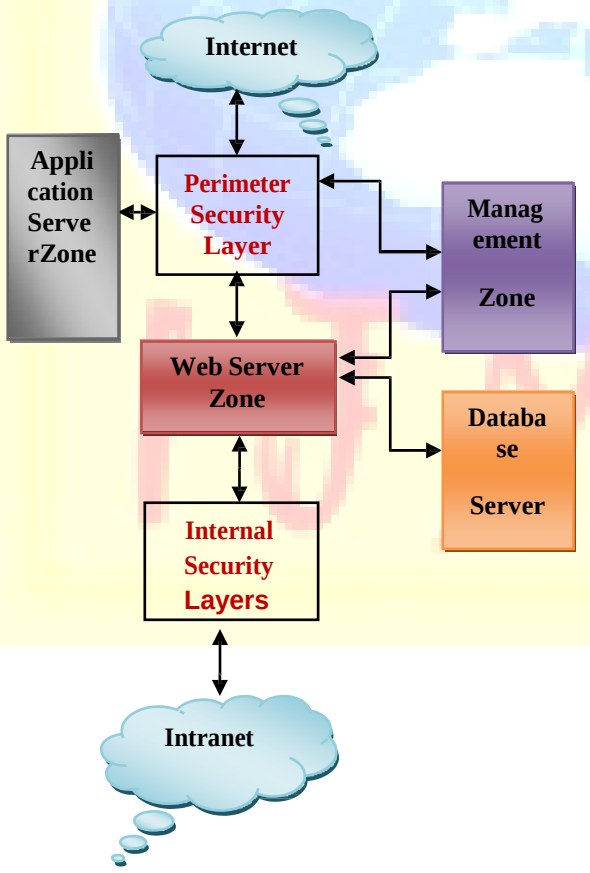


Figure 1. Simple network security architecture for organization

This architecture consist of total six fields such as Database server zone, Application server zone, Web server zone, Internet security layer, Intranet, Internet, Perimeter security layer.

Internet is relatively short, its growth has been dynamically explosive. The Internet users are increases in worldwide day by day. The Internet is a worldwide collection of networks that links together millions of computers by various means, such as modems, fibre optic lines and various servers. It provides connections to various businesses, the government, industries, educational institutions, and individuals. Each of these organizations has become increasingly dependent on networks and distributed computing and processing systems.

Intranets provide organizations with tremendous ability to communicate, but they do not use any traditional model which use for communication. While you can publish employee information on the Intranet, the system empowers employees and departments themselves to become publishers and communication facilitators. An Intranet allows anyone in the company to tap into the entire organization's intellectual capital, rather than the limited circle of fellow employees with whom most employees have day-to-day contact.

Web server zones are responsible for interaction with the user , the **application server zone** perform data processing and database server zone provide data storage. Those server which has same type that provides the various services and that services are separated and located in different zones. **Internet** does not have authority for the direct accessing the application and database server. **Web server zone** access only the **application server zone** and **application server zone** access only **database server zone.** The main reason behind designing this architecture is to stop the various attacks from hackers and crackers in **web server zone** .There are two security layer such as **Perimeter security layer** and **Internet security layer. Perimeter security layer** consist of routers providing first layer of protection which has dedicated security devices such as firewall, VPN and other required devices. **Internet security layer** consist of some dedicated security devices such as firewall, IPS and other required security devices.

4. Advantages of network security architecture

- Isolation of low-trust network areas, which can be potentially used to launch attacks against strategic IT system resources
- Limitation of the security breach scope to one system or network segment as well as limiting the incident spreading to other systems
- Accurate network access control to IT system resources as well as monitoring and auditing resource usage and management
- Quick identification of IT systems security incidents based on the events detected in the network areas, these events should not occur.
- Cost optimization by an appropriate IT resource location and segmentation, and deployment of adequate safe guards for requirement compliance.

5. Need of network security: -

The need for network security is quite obvious. There are criminal activities in every field, computers being no exception. People like to store private information on computers. If a criminal was successful in his attack onto your network, they would successfully retrieve the information on that computer. By addressing their security issues, you not only will be able to make a more informed decision when choosing a protocol but you will also understand all these efforts and fuzz on security alternatives i.e.

- **FIREWALL.**
- **CRYPTOGRAPHY.**
- **VIRTUAL PRIVATE NETWORK**

becomes necessary.

5.1 Firewall

A firewall is the entry gate in front of many group of machines. It's main function is to control communication between machines. At the time of this communication over the internet a stream of data send in both directions. Firewall comprises of a application software that can reside in a communication router, server or some other device. Firewall are designed to keep unwanted and unauthorized traffic from an unprotected network like the Internet out of a private Network like your LAN/WAN, yet still allowing you and other user of your local network to access Internet Services.

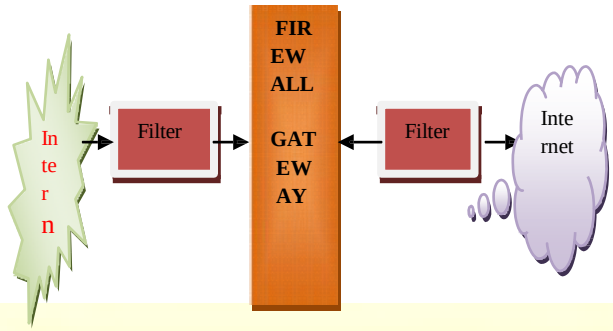


Figure 2.Basic purpose of the firewall

The purpose of firewall, or a security gate, is to provide security to those components inside the gate, as well as control of who (or what) is allowed to get into this protected environment, as well as those allowed to go out. It works like a security guard at a front door, controlling and authenticating who can or cannot have access to the site.

5.1.1Merits of firewall :-

1. One of the primary goal of the firewall is to protect each site against **hackers**.

2. It's setup provide controllable filtering traffic on, the network and allowing restricted access to certain Internet port numbers.

3. Firewall is also used to protect against unauthenticated interactive login from the outside world.

4. With the firewall, we can also protect our site from the arbitrary connections and can also be the set up tracing tools.

5.1.2 De-Merits of firewall :-

1. It does not protect your site against connection bypassing.

2. A firewall is not infallible; its main purpose is to increase the security. If you have very valuable information LAN, your server should not be connected to first place.

3. If you have a web server inside your internal LAN then watch for internal attacks, as well as to your corporate server. But firewall can do nothing a about threats coming from inside of the organization.

5.2 Cryptography

The simple meaning of Cryptography is conversion of simple message into the unreadable format so that only known or authorized person can read it and to avoid the alteration of message. It is an art and science of keeping messages and information secure from uninterested third party i.e. when a sender sends a message to a receiver it is send in such a way that no one except sender and receiver can recognize the message and alter the message. Cryptography is another way to provide security to a network. Cryptography allows two parties to exchange sensitive information in a secure manner. Encryption scrambles the information so that only the intended recipient recovers the original information by decrypting it .Fig. shows that sender can send the simple message to the Encryptor, Encryptor can convert that simple message into encrypted form and this message is now send to the Decryptor. Decryptor can convert this encrypted message into decrypted message and then this message is send to Receiver.

Encrypted Decrypted

message message

emails. It is also use for file transfer, remote login and remote job entry.

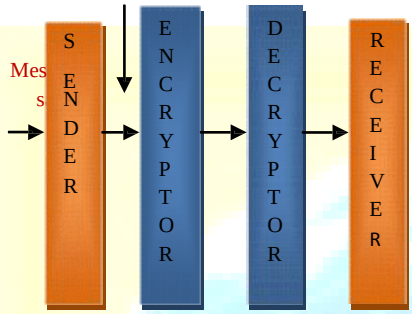
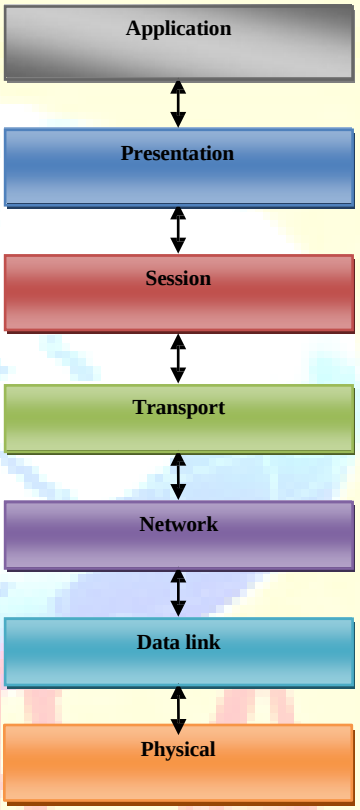


Figure 3. Simple representation of cryptography



5.3 Virtual private network

A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network through the security procedures. It is one solution to establishing long-distance and/or secured network connections. VPNs is mostly used and implemented by businesses or organizations rather than single user, but it is also use for home network. As compared to other technologies, it gives various several advantages, particularly it is beneficial for wireless local area networking.

5. OSI Layer Model

The OSI, or Open System Interconnection, model defines a networking framework to implement protocols in seven layers. This article explains the 7 Layers of the OSI Model.The OSI, or Open System Interconnection, model defines a networking framework to implement protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Application Layer (Layer 7)

Application layer provide a service that directly support the end user of the network. The application layer is basically a collection of various protocols for various commonly used application such as

Figure 4. OSI Layer Model Presentation Layer (Layer 6)

The purpose of this layer is to represent message information. Presentation layer is concerned with the representation of data i.e being exchanged. This can include conversion of the data between different format data compression and encryption.

Session Layer (Layer 5)

The purpose of the session layer is to provide a the means by which presentation entities can organize and synchronize their dialogue and manage their data exchange. The dialogue control is useful for sending and receiving message.

Transport Layer (Layer 4)

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. Another job of the transport layer is to provide a site to site

communication and hide the all the data or detail of communication. The transport layer accept the message of arbitrary length from the session layer and then segment them into packet at destination. Some packets are lost on the way from the sender to the receiver.

Network Layer (Layer 3)

The Network Layer is responsible for setting the logical path between two sites for communication. This layer also provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. It encapsulate the frame into packets that can transmitted from one site to another using a high level of addressing and routing scheme. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link Layer (Layer 2)

The physical layer simply transmit the data from the senders site to the receiver site as raw data. It is responsibility of data link layer to detect and correct any error in the transmitted data. Since the only physical layer concerned with the raw data ,the data link layer partitioned into the frame so that error detection and correction performed for each frame. The data link layer also perform the operation of flow control of frames.

Physical Layer (Layer 1)

The physical layers responsibility is to transmit the raw data between two sites i.e. may convert the sequence of binary bit into electrical signal, light signal or electromagnetic signal depending upon the whether two sites are on cable circuit, fibre optic circuit or microwave circuit. In short the physical layer deal with mechanical, electrical, procedural and functional characteristic of transmission of raw data between two sites.

6. Future work

Although Network security is very important in today's growing world of networking. Some powerful software may be developed which common for all field which protecting the physical infrastructure and gives confidence to the user including strong detectation and preventation power. In future some other software are developed for the home network security. Some strategy which encrypting the communication between the parties. The future of network security might be far from clear-cut.

7. Conclusion

Network security is prime concept in today's world of networking. Everyone should about security with their advantages, disadvantages and also preventation. It is an important and critical issue that all computer systems need to have implemented some sort of security control. Without having security, sensitive information can be easily gained by hackers or crackers or any other unauthorised person so it is important that we determine, prevent, detect, and correct security issues.

8. References

[1]W. Cheswick and S. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 1994.

[2]Joshua Backfield, John Bambenek, "Network Security Model", SANS Institute, 2008

[3]Virtual Private Networks http://technet.microsoft.com/enus/network/bb545442.aspx

.

[4] J.P. Holbrook, J.K. Reynolds. ``Site Security Handbook." RFC 1244.

[5] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously,"

Computer, vol.31, no.9,pp.24-28, Sep 1998

[6] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," *Communications, 2008. ICC '08.IEEE International Conference on*, pp.1469-1473, 19-23May 2008.

[7]SecurityOverview,"www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[8] Network Security Architecture
By Mariusz Stawowski – ISSA member, Poland Chapter

[9] ISO/IEC 18028-2 (ITU X.805) Network security architecture. 2006ISO/IEC.

[10]http://www.engpaper.com/free-research-papers- network-security-11.htm

[11]http://www.engpaper.com/free-research-papers- network-security-02.htm

[12]Cooper, P.S. (February 1996). Network Security Management With Firewalls [DOE Information Security ConferencePresentations]. Retrieved on March 6 2005 from http://doeis.llnl.gov/ConferenceProceedings/DOECompSe c96/firewall.pdf

[13]Al-Shaer, S.E. & Hamed, H.H. Design and Implementation of Firewall Policy Advisor Tools.
Retrieved on March 3, 2005 from http://facweb.cs.depaul.edu/research/TechReports/TR04-011.pdf.

[14]Protecting and Connecting the Distributed Organization – A Comprehensive Security and
VPN Strategy. Retrieved February 15, 2005, from https://partners.mysonicwall.com/WhitePaper/Download Center/WhitePapers.asp