A Framework For Network Stability And Security

Dr. R.K.P. Yadav*, Akhilesh Kumar, Rahul Ranjan*****

ABSTRACT

Computer networks were primarily used by university researches for sending email, and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem. In the following sections, we will study network security from several angles, point out numerous pitfalls, and protocols for making networks more secure.

Network security problems can be divided roughly into four intertwined areas: secrecy, authentication, Non-repudiation, and integrity control. Secrecy has to do with keeping information out of hands of authorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal.

In the network layers, firewalls are installed to keep packets in or keep packets out. In the transport layer entire connections can be encrypted, end-to-end, that is, process to process. To tackle these problems, the solutions must be in the application layer, which is why these are being studied in this paper.

Network security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. When people use the Internet, they have certain expectations. They expect confidentiality and the data integrity. They want to be able to identify the sender of a message. They want to be able to prove that a message has in fact sent by a certain sender even if the sender denies it.

INTRODUCTION

What is a Network?

A network has been defined[1] as any set of interlinking lines resembling a net, a

* Dept. of Mathematics P.G. Centre Gaya College Gaya (M.U. Bodh Gaya, principalgcgaya@yahoo.com

** Research Scholar (M.U. Bodh Gaya, akhilesh2gaya@rediffmail.com

*** Research Scholar (M.U. Bodh Gaya)

network of roads | | an interconnected system, a network of alliances." This definition suits our purpose well: a computer network is simply a system of interconnected computers. How they're connected is irrelevant, and as we'll soon see, there are a number of ways to do this.

The ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them. Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together.

An easy way to look at this is to compare this model with something we use daily: the telephone. In order for you and I to talk when we're out of earshot, we need a device like a telephone. (In the ISO/OSI model, this is at the application layer.) The telephones, of course, are useless unless they have the ability to translate the sound into electronic pulses that can be transferred over wire and back again. (These functions are provided in layers below the application layer.) Finally, we get down to the physical connection: both must be plugged into an outlet that is connected to a switch that's part of the telephone system's network of switches.

If I place a call to you, I pick up the receiver, and dial your number. This number specifies which central office to which to send my request, and then which phone from that central office to ring. Once you answer the phone, we begin talking, and our session has begun. Conceptually, computer networks function exactly the same way.

It isn't important for you to memorize the ISO/OSI Reference Model's layers; but it's useful to know that they exist, and that each layer cannot work without the services provided by the layer below it.

TCP / IP:

TCP/IP (Transport Control Protocol/Internet Protocol) is the ``language'' of the Internet. Anything that can learn to ``speak TCP/IP'' can play on the Internet. This is functionality that occurs at the Network (IP) and Transport (TCP) layers in the ISO/OSI Reference Model. Consequently, a host that has TCP/IP functionality (such as Unix, OS/2, MacOS, or Windows NT) can easily support applications (such as Netscape's Navigator) that uses the network.

Services for security:

The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. These are :

1. **Confidentiality:** Ensure that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing displaying and other forms of disclosure, including simply revealing the existence of an object.
2. **Authentication:** Ensure that the origin of a message or electronic document is correctly with an assurance that the identity is not false;
3. **Integrity:** Ensures that only authorized parties are able to modify computer systems assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages.
4. **Non-repudiation:** Requires that neither the sender nor the receiver of a message is able to deny the transmission.
5. **Access control:** Require that access to information resources may be controlled by or for the target system.
6. **Availability:** Require that computer systems assets be available to authorized parties when needed.

Attacks:

Attacks on the security of a computer system or network are best characterized by viewing the function of a computer system as provided information. This normal flow is depicted in figure 1

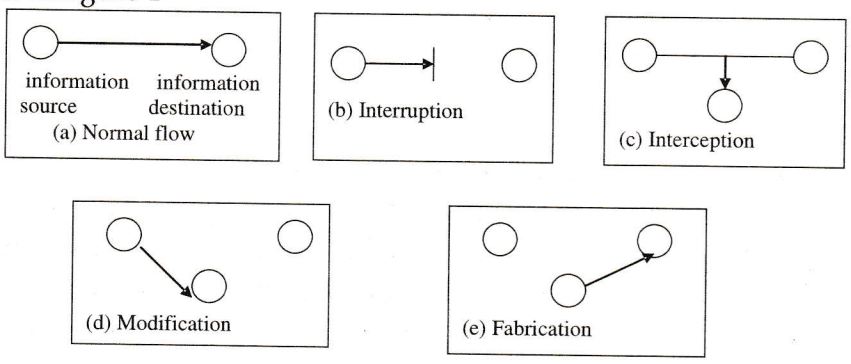


Fig-1 : Categorization of these attacks is passive attacks and active attacks.

Passive attacks: In this, the goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

Active attacks: These attacks involve some modification of the data stream or the creation of false stream and can be sub divided into 4 categories: Masquerade, Replay, Modification of messages, and denial of service.

TYPES AND SOURCES OF NETWORK THREATS

Denial-of-Service

DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

Unauthorized Access

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

Where Do They Come From?

How, thugh, does an attacker gain access to your equipment? Through any connection that you have to the outside world. This includes Internet connections, dial-up modems, and even physical access. (How do you know that one of the temps that you've brought in to help with the data entry isn't really a system cracker looking for passwords, data phone numbers, vulnerabilities and anything else that can get him access to your equipment?)

In order to be able to adequately address security, all possible avenues of entry must be identified and evaluated. The security of that entry point must be consistent with your stated policy on acceptable risk levels.

Hope you have backups

This isn't just a good idea from a security point of view. Operational requirements

should dictate the backup policy, and this should be closely coordinated with a disaster recovery plan, such that if an airplane crashes into your building one night, you'll be able to carry on your business from another location. Similarly, these can be useful in recovering your data in the event of an electronic disaster: a hardware failure, or a breakin that changes or otherwise damages your data.

Don't put data where it doesn't need to be

Although this should go without saying, this doesn't occur to lots of folks. As a result, information that doesn't need to be accessible from the outside world sometimes is, and this can needlessly increase the severity of a break-in dramatically.

Avoid systems with single points of failure

Any security system that can be broken by breaking through any one component isn't really very strong. In security, a degree of redundancy is good, and can help you protect your organization from a minor security breach becoming a catastrophe.

FIREWALLS

A firewall provides a strong barrier between a private network and the Internet. Firewalls can be set to restrict the number of open ports , what type of packets are passed through and which protocols are allowed through . On a should have a good firewall in place before implementing a VPN , but a firewall can also be used to terminate the VPN sessions .

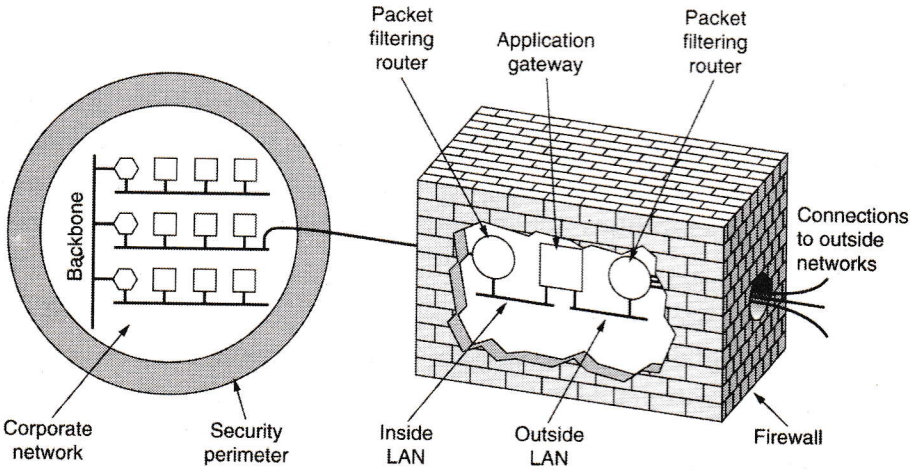


Fig-2: A fire wall consisting of two packet filters and an application gateway

As we've seen in our discussion of the Internet and similar networks, connecting an organization to the Internet provides a two-way flow of traffic. This is clearly undesirable in many organizations, as proprietary information is often displayed freely within a corporate intranet (that is, a TCP/IP network, modeled after the Internet that only works within the organization).

In order to provide some level of separation between an organization's intranet and the Internet, firewalls have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

Types of Firewalls

There are three basic types of firewalls, and we'll consider each of them. These are :

Application Gateways

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server. This software runs at the Application Layer of our old friend the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy, and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic.

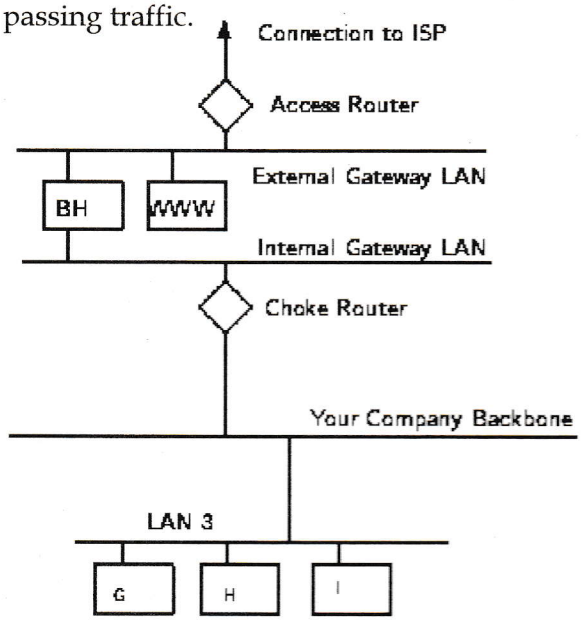


Fig-3 : A sample application gateway

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 it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice-versa. There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer).

Hybrid Systems

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

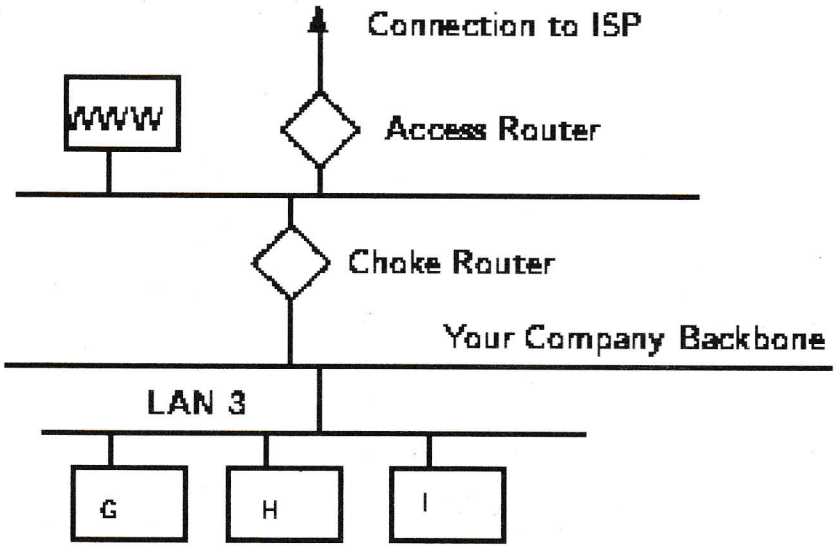


Fig-4 : A sample packet filtering gateway

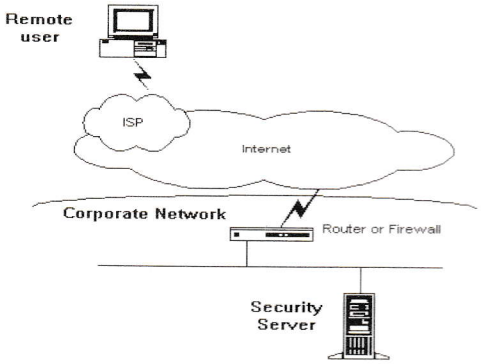
NETWORK SECURITY CAN BE DONE BY VARIOUS METHODS.

1. Virtual Private Network: (VPN) :

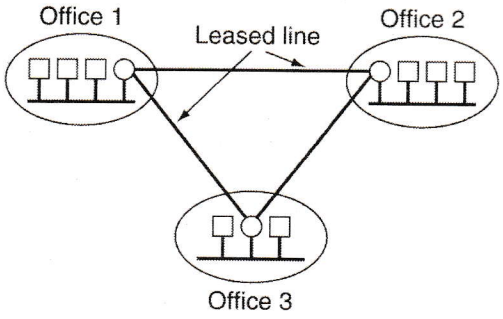
A virtual private network (VPN) is a way to use a public telecommunication infrastructure , such as the Internet , to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities , but at a much lower cost

Implementation of network security by VPN.

Step 1. - The remote user dials into their local ISP and logs into the ISP's network as usual.

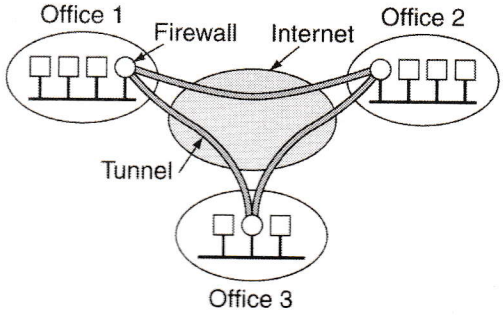


Step 2. - When connectivity to the corporate network is desired, the user initiates a tunnel request to the destination Security server on the corporate network. The security server authenticates the user and creates the other end of tunnel.



(a)

Fig : a) A leased line private network



(b)

Fig : b) A virtual private network

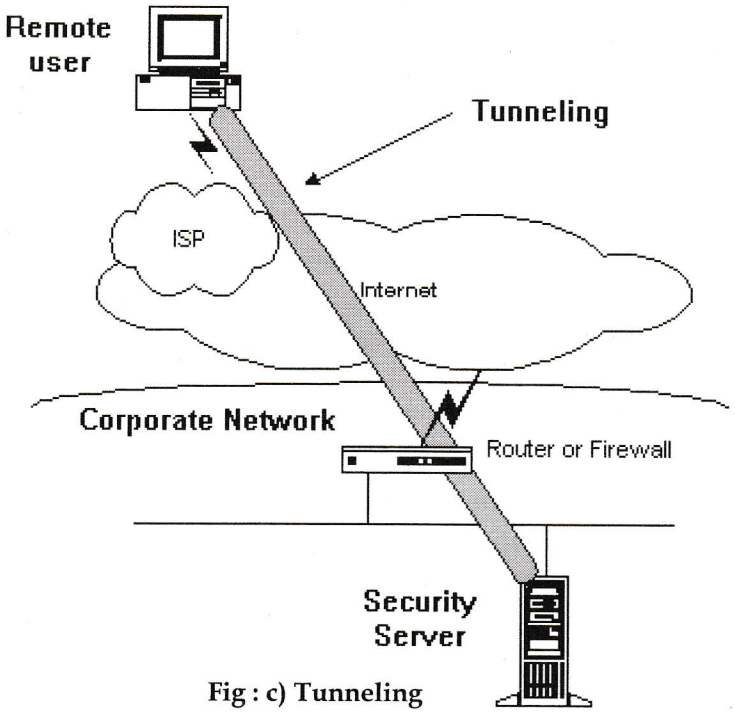


Fig : c) Tunneling

Step 3. - The user then sends data through the tunnel which encrypted by the VPN software before being sent over the ISP connection.

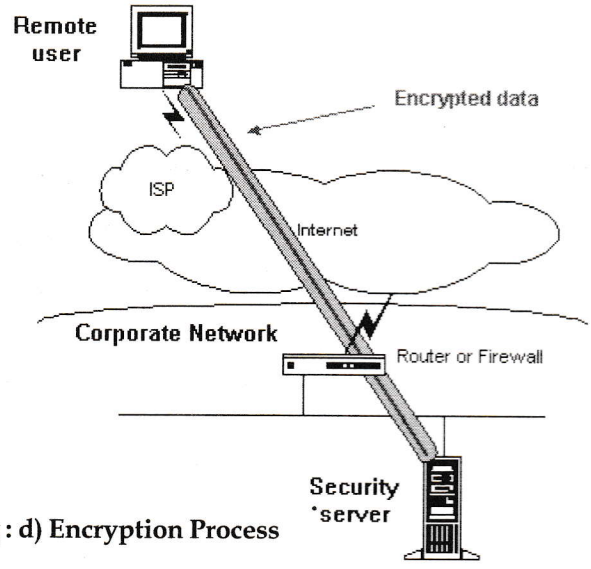


Fig : d) Encryption Process

Step 4. - The destination Security server receives the encrypted data and decrypts. The Security server then forwards the decrypted data packets onto the corporate network. Any information sent back to the Remote user is also encrypted before being sent over the Internet.

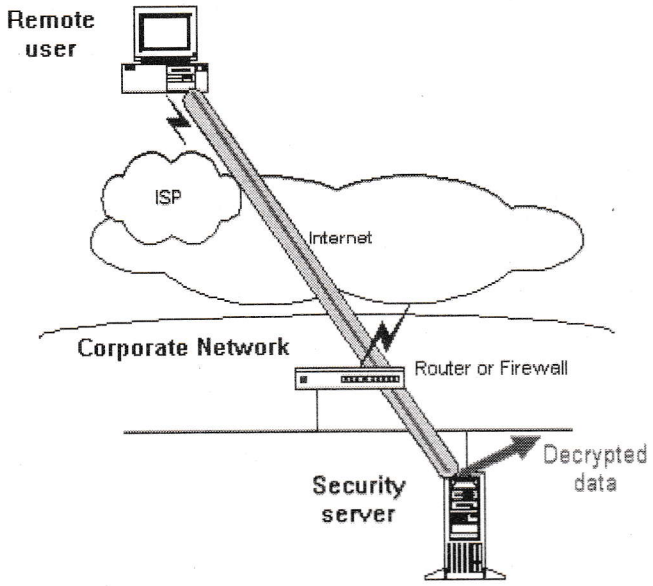


Fig : e) Decryption Process

IPSee :

Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication . IPSec has two encryption modes : tunnel and transport. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. Only systems that are IPSec compliant can take advantage of this Protocol . Also , all devices must use a common key and the firewalls of each network must have very similar security policies set up. IPSec can encrypt data between various devices , such as :

Router to router, Firewall to router, PC to router, PC to server

A software firewall can be installed on the computer at your home that has an Internet connection . This computer is considered a gateway because it provides the only point of access between the network and the Internet .

CONCLUSIONS

Security is a very difficult topic. Everyone has a different idea of what ``security'' is,

and what levels of risk are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know why what's been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.

Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

REFERENCES

[1] The New Lexicon Webster's Encyclopedic Dictionary of the English Language. New York: Lexicon.

[2] R.T. Morris, 1985. A Weakness in the 4.2BSD Unix TCP/IP Software. Computing Science Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey.

[3] S.M. Bellovin. Security Problems in the TCP/IP Protocol Suite. Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989.