© 2014 IJIRT | Volume 1 Issue 6 | ISSN : 2349-6002

# NETWORK SECURITY

## Flexible approach to improve system reliability

Sheena Batra, Rakesh Sondal
Dronacharya College of Engineering, Guragon

***Abstract*— Network Security refers to a documentation giving users an overview of the security risks and countermeasures associated with internet connectivity. Basically it refers to an organization's strategy and provisions for ensuring the security of all the network traffic and its assets. Network security is rapidly gaining prominence because of excessive threats to our networks. So it demands very strong defensive mechanism system be it for small or a bigger network. Network security increases work productivity, reduces costs, prevents unauthorized access to our data and its misuse. Thus, now there is a growing realization among all, i.e., organizations as well as home users to secure their network from any kind of threats. This paper presents a replicated approach to enhance and secure the network with virtual lockstep, making systems reliable on the network. To secure a network we must use control strategies like firewall solutions, content gateway security, integrated VPN, firewalls, etc.**

### I. Introduction

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network
comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as"Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not
threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet. The vast topic of network security is analyzed by
researching the following:
1. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of internet attacks and security methods
4. Security for networks with internet access
5. Current development in network security hardware and software
Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand
where network security is heading.

### II. network security

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security
methods that can be easily implemented. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed
process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a welldeveloped
process. There isn't a methodology to manage the complexity of security requirements.Secure network design does not contain the same advantages as network design.When considering network security, it must be emphasized that the whole network is secure.
Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the
communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network

is just as important as securing the computers and encrypting the message. When developing a secure network, the following
need to be considered :

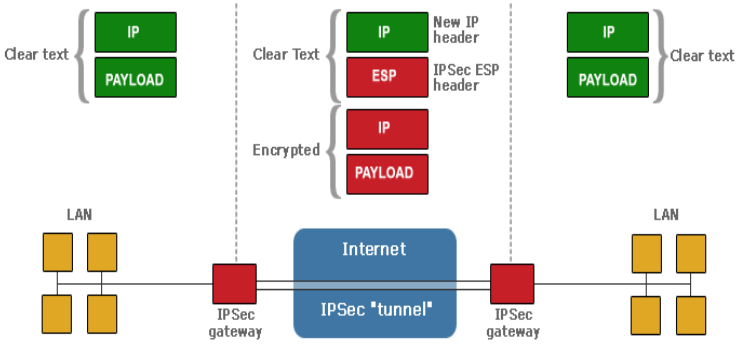
1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanism, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools.“Intranets” are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in thnetwork. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself. The types of attacks through the internet need to also be studied to be able to detect and guard
against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of
packets that are introduced to cause problems for the following reasons:

• To consume resources uselessly
• To interfere with any system resource’s intended function
• To gain system knowledge that can be exploited in later attacks

## III. SECURITY TIMELINE

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s. Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II. In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defense began the ARPANet, which gains popularity as a conduit for the electronic exchange of data and information. This paves the way for the creation
of the carrier network known today as the Internet. During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers. During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414
gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy’s crime of stealing information from military computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000
vulnerable computers connected to the Internet. Based on concerns that the Morris Worm ordeal could be replicated, the Computer Emergency Response Team (CERT) was created to alert computer users of network security issues. In the 1990s, Internet became public and the security concerns increased tremendously.Approximately 950 million people use the internet today worldwide [3]. On any day, there are approximately 225 major incidences of a security breach [3]. These security breaches could also result in monetary losses of a large degree. Investment in proper security should be a priority for large organizations as well as common users.




## IV. SECURITY IN DIFFERENT NETWORKS

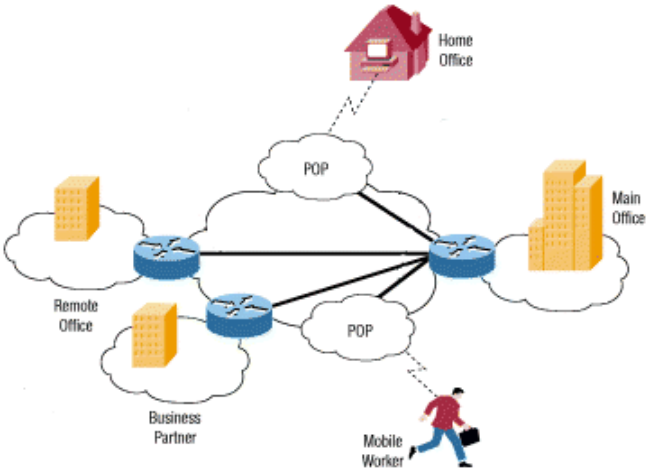
The businesses today use combinations of firewalls,encryption, and authentication mechanisms to create “intranets” that are connected to the internet but protected from it at the same time. Intranet is a private computer

network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties. There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs). Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. But for broader data sharing, it might be better to keep the networks open, with these safeguards: 1. Firewalls that detect and report intrusion attempts

2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of email attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates It was mentioned that if the intranet wanted access

to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines or a newer approach of VPN can be utilized. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual"

connections routed through the Internet from the company's private network to the remote site or employee. Figure below is a graphical representation of an organization and VPN network.




## V. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing

in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assists in understanding current development and projectingthe future developments of the field

**1. Hardware Developments**

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security. The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. Each workstation requires some software support for biometric identification of the user as well as,

depending on the biometric being used, some hardware device. The cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next

step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device.

**2. Software Developments**

The software aspect of network security is very vast. It includes firewalls, antivirus, vpn, intrusion detection, and much more. The research development of all security software is not feasible

to study at this point. The goal is to obtain a viewof where the security software is heading based on emphasis being placed now.

The improvement of the standard security software still remains the same. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analyzing attack patterns in order to create smarter security software.

**FUTURE TRENDS IN NETWORK SECURITY**

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system. The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security

technology that is being used today with minor adjustments.

## VI. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the

current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near

future. The network security field may have to evolve more rapidly to deal with the threats further in future.

## REFRENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *Computer*, vol.31, no.9

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

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

[4] Molva, R., Institut Eurecom,"Internet Security Architecture," in *Computer Networks & ISDN Systems Journal*, vol. 31, pp. 787-804, April 1999