ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1920-1927

SECURITY MODEL FOR COMPUTER NETWORK BASED ON CLUSTER COMPUTING

Satish Kumar Thalod, Ram Niwas

M.Tech (CSE) – Part Time, Ch. Devi Lal University, Sirsa [1]

Teaching Associate (CSA Department), Ch. Devi Lal University, Sirsa [2]

Abstract
Network security is a complicated subject, historically only tackled by well-trained and experienced experts. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. A computer cluster may be a simple two-node system which just connects two personal computers, or may be a very fast supercomputer. Although a cluster may consist of just a few personal computers connected by a simple network, the cluster architecture may also be used to achieve very high levels of performance. A cluster computing security model is a scheme for specifying and enforcing security policies. This paper proposes a security model for a computer network based on cluster computing architecture by using various tools available in TCP/IP security model.

KEYWORDS: TCP/IP, Security Model, Cluster Computing, Computer Network

INTRODUCTION TO NETWORK SECURITY

A simple network can be constructed using the same protocols and such that the Internet uses without actually *connecting* it to anything else. Such a basic network is shown in the following figure:

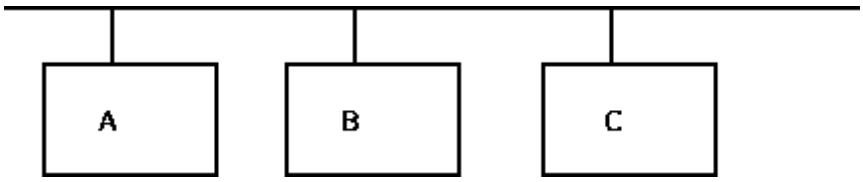

Figure 1: A Simple Local Area Network

Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. The evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly

exercised attacks causing damage or committing theft. The Internet continues to grow exponentially. As personal, government and business-critical applications become more prevalent on the Internet, there are many immediate benefits. A computer network is simply a system of interconnected computers. The Internet is the world's largest network *of networks*. When you want to access the resources offered by the Internet, you don't really connect to *the* Internet; you connect to a network that is eventually connected to the *Internet backbone*, a network of extremely fast (and incredibly overloaded!) network components. The Internet is a network of *networks*, not a network of hosts.

Various types of network security threats are:

- ✓ Viruses
- ✓ Trojan Horse Programs
- ✓ Vandals
- ✓ Attacks
- ✓ Data Interception
- ✓ Social Engineering
- ✓ Unauthorized Access Executing
- ✓ Commands Illicitly
- ✓ Denial-of-Service (DOS) Attack
- ✓ Confidentiality Breaches

Various types of network security tools are:

- ✓ Antivirus Software Packages
- ✓ Secure Network Infrastructure
- ✓ Encryption Techniques
- ✓ Backup Techniques
- ✓ Updated Operating Systems
- ✓ Updated Web Browsers

TCP/IP: THE LANGUAGE OF INTERNET

Transmission Control Protocol / Internet Protocol (TCP/IP) was developed in 1978 and driven by Bob Kahn and Vint Cerf. Today, TCP/IP is a language governing communications among all computers on the Internet. TCP/IP is a combination of two separate protocols, TCP and IP that are used together. The Internet Protocol standard dictates how packets of information are sent out over networks. IP has a packet-addressing method that lets any computer on the Internet forward a packet to another computer that is a step (or more) closer to the packet's recipient. The Transmission Control Protocol ensures the reliability of data transmission across Internet connected networks. TCP checks packets for errors and submits requests for re-transmissions if errors are found; it also will return the multiple packets of a message into a proper, original sequence when the message reaches its destination.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

Different security tools available in TCP/IP Model are:

Application Layer: Kerberos, S/MIME, PGP, SET
Transport Layer: SSL/TLS
Internet Layer: IPSec
Network Interface Layer: CheckSum

Kerberos is an Authentication service designed for use in a Distributed Environment. Kerberos makes use of a trusted third part Authentication service that enables client and server to establish authenticated communication.

***Secure / Multipurpose Internet Mail Extension (*S/MIME)** is a security environment to the MIME internet E-Mail format standard, based on technology from Rivest Shannon Algorithm data security.

Pretty Good Policy (PGP) provides Confidentiality and Authentication service that can be used for electronic mail and file storage application. PGP provide five services: Authentication, Confidentiality, Compression, E-Mail Compatibility, and Segmentation.

Secure Electronic Transaction (SET) is an open Encryption and security specification designed to protect credit card transaction on the internet.

***Secure Socket Layer* (SSL)** makes use of TCP to provide reliable end to end secure services. SSL is combination of four Protocols: SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Specification Protocol, and SSL Alert Protocol. Application layer security is achieved by all these facilities.

IPSec provide security to IP layer. It provides the capability to secure communication across a LAN and across the internet. IPSec encompasses three functional areas Authentication, Confidentiality, Key Management. Authentication Header (AH) protocol, Encryption Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP) are the working protocols of IPSec.

CheckSum is a tool which is used to confirm Authentication of Sending Data. It is used to provide authentication services for various server and client terminals over the computer network.

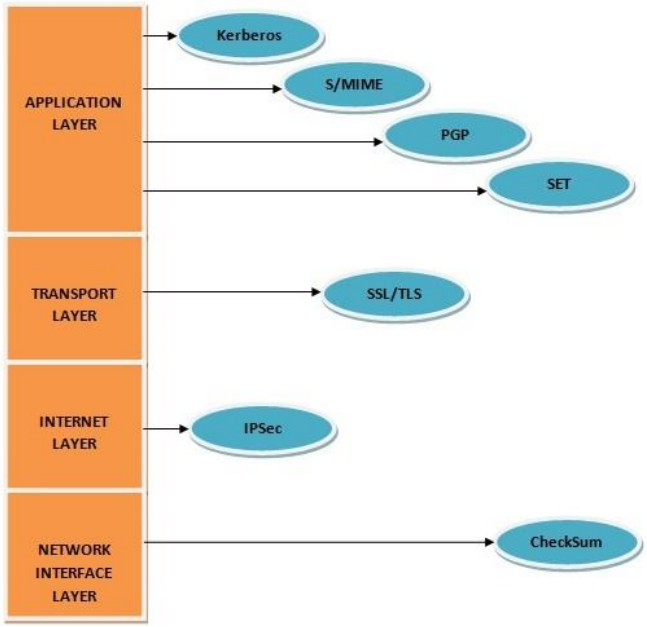

Figure 2: Security Tools available at different layers of TCP/IP Model

Every security tool available in TCP/IP Model has support to different types of security features. These security features are defined as follows:

- ✓ User Validation
- ✓ Access Permission
- ✓ System Discretion
- ✓ Packet Seclusion
- ✓ Message Integrity
- ✓ Channel Reliability
- ✓ Single User Access
- ✓ Firewall Prevention
- ✓ Secure Network Signing
- ✓ Internet Protocol Addressing
- ✓ Network Authentication
- ✓ Server & Client Authorization

BASICS OF CLUSTER COMPUTING

A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks. Clusters are usually deployed to improve performance and/or availability over that of a single computer, while typically being much more cost-effective than single computers of comparable speed or availability. In a computer system, a cluster is a group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing. Cluster computing is the technique of linking two or more computers into a local area network in order to take the advantage of parallel processing. A cluster computing security model is a scheme for specifying and enforcing security policies. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, or no particular theoretical grounding at all. A cluster is a type of parallel or distributed processing system, which consists of a collection of interconnected stand-alone computers working together as a single integrated computer resource.

We divided the available cluster computing architecture into four different levels, as per the availability of various security tools in TCP/IP Model. On each of these levels, we check for different security features needed to make cluster computing architecture secure. Then we apply various security tools available in TCP/IP Model on different levels of cluster computing architecture.

The four different levels defined over cluster computing architecture are:

1. End User External Level
2. Coherent Rational Level
3. In-House Hardware Level
4. System Connection Level

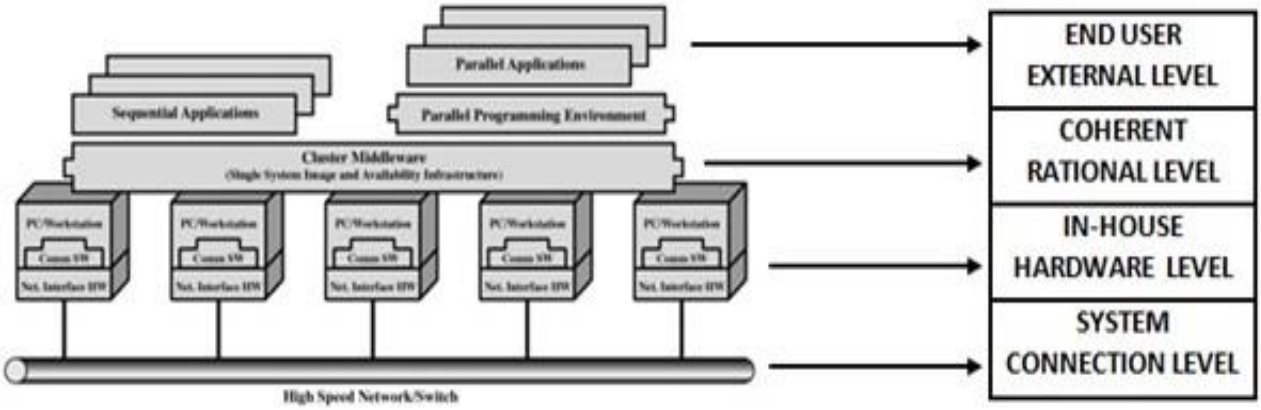

Figure 3: Various Levels defined over Cluster Computing Architecture

PROPOSED SECURITY MODEL

Security is one of the most important factors that need to be considered during clustering of many computers in a high performance computing system, especially when they are implemented through the internet, because there is possibility of the network to be susceptible for any kind of attack. The attacks to clustering of nodes could come in different forms – it could be as simple as a virus wherein its sole purpose is to destroy files or could be a very powerful spyware that can easily hijack the controls of nodes for malicious purposes. Those who want to implement clustering have to make sure the nodes, the connections and the implementation of nodes when it comes to handling workload could be optimized for security.

It only takes a single security flaw to destroy the entire clustering configuration. Whenever a network opens up a connection to its administrator, it automatically opens itself to different forms of attacks. This is also possible for users who try to access the nodes and stores data. In gist, there is always a possibility of attack whenever an interaction happens with the client and the server. This is practically the "security nightmare" in clustering since interaction will always happen which means the nodes are always susceptible to different attacks.

The proposed security model for computer network based on cluster computing consists of various security tools available in TCP/IP Model. Every tool has its own security features which make the system secure. We apply these security tools with their security features on different levels of cluster computing architecture, to make it a secure high performance computing system.

TCP/IP Model	Security Tools	Security Features	Cluster Computing Architecture Levels
Application Layer	Kerberos S/MIME PGP SET	User Validation Access Permission System Discretion	End User External Level
Transport Layer	SSL/TLS	Packet Seclusion Message Integrity Channel Reliability Single User Access Firewall Prevention	Coherent Rational Level
Internet Layer	IPSec	Secure Network Signing Internet Protocol Addressing	In-House Hardware Level
Network Interface Layer	CheckSum	Network Authentication Server & Client Authorization	System Connection Level

Figure 4: Proposed Security Model for Computer Network based on Cluster Computing

CONCLUSION

Computer network based on cluster computing is a good example of high performance computing systems. Requirement of security in cluster computing systems is not ignorable. This paper presents a model which applies various security tools available in TCP/IP model on different defined levels of cluster computing architecture for various types of security features. Every security tool is having their own constraints like, number of users in communication, intrusion detection and policy management. The result defined in this model satisfies various security requirements for a computer network based on cluster computing architecture. The proposed model also provides a better and safe interface to make communication in between various users, system and network resources. No another existing or old model provides this type of results to maintain security for computer network based on cluster computing architecture.

REFERENCES

[1] Chris Hare and Karanjit Siyan, et. al. "Internet Firewalls and Network Security", System Security Consulting, Second Edition, Northern Telecom Ltd. (Nortel), 1986.

[2] Jeffrey S. Vetter, Frank Mueller et. al. "Communication Characteristics of Large-Scale Scientific Applications for Contemporary Cluster Architectures", Proceedings, 20th annual International Symposium Computer Architecture, 1993.

[3] Zhe Fan, Feng Qiu, Arie Kaufman, Suzanne Yoakum-Stover et. al. "GPU Cluster for High Performance Computing", In Proceedings of the 29th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH), 2002.

[4] Steven M. Bellovin et. al. "Security Problems in the TCP/IP Protocol Suite Vol. 2", Computer Communication Review, Vol. 19, No. 2, in April, 1989.

[5] Kay Connelly, Andrew A. Chien et. al. "Breaking the Barriers: High Performance Security for High Performance Computing", IEEE Mass Storage Conference, 2001.

[6] Chee Shin Yeo, Rajkumar Buyya, Hossein Pourreza, Rasit Eskicioglu, Peter Graham and Frank Sommers et. al. "Cluster Computing: High-Performance, High-Availability, and High-Throughput Processing on a Network of Computers", Cluster Computing, vol. 6, no. 4, Oct. 2003, pp. 287-297.

[7] Mark Baker et. al. "Cluster Computing White Paper", In Proceedings of EuroPar'99, LNCS 1685, August 31-September 3, 1999, Toulouse, France.