Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Proposed Model for IP Address Security

Pawan Kr. Chaurasia
Department of Information Technology
Babasaheb Bhimrao Ambedkar University,
(A Central University), Vidya Vihar, Raebareli Road, Lucknow- 226025 INDIA

Abstract —From last two to three decade internet users are increased in exponential form. It is very difficult to secure data when two users want to communicate through Internet. When we share information and resources among various users on internet, then networking is required to implement. Today hacking is the major problem with internet user. When user shared information or data then they share the IP address also between two users. It is mandatory to provide strong security on IPV4 address to secure data in the form of XXX.YYY.ZZZ.RRR. IP addresses are binary numbers, which are usually stored in text files. IP address is classified into various classes. IP address is secured on IPV4. A class model is proposed to secured data on internet through IP address. Through RSA algorithm, it is tested and verified, IP address on sender end and receiver end are same during the share of information between two users.

Keywords – IPV4, Security, RSA, Class, IP, UML.

I. INTRODUCTION

As network is expanded day-by-day, Internet Protocols are increased in a same manner. Different mechanism and devices are used and a lot of research work is carried out in this area. An Internet Protocol (IP) address is a network address which is unique for every host connection on an IP network. It is numerical values which is assigned to each device and are used in computer network for data communication. It is a transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocol. It provides host-to-host communication between the users on the internet. There are two versions of Internet Protocol which are basically used, IPV4 (Internet protocol Version 4) and IPV6 (Internet Protocol Version 6).

IPV4 was first developed in 1970 and it is functionally published in 1981. With huge demand it is increased with time and assigned the IP address as per requirement. IP address is a 32 bit binary number which represent 4 decimal values, each representing 8 bits, in the range 0 to 255 separated by decimal points. This is known as "dotted decimal" notation. Every IP address consists of two parts, one identifying the node and one identifying the network. The Class (A, B, C, D, E) of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address [1]. With the growth of the Internet and its possible extension, IPv6 increases the IP address from 32 bits to 128 bits to support more levels of the addressing hierarchy but the present work is only confine to IPV4.

UML is a large modeling language for visual purpose and is used to specify, construct, visualize and document the software [2]. The appearance of UML (Unified Modeling Language) and its being accepted as standard by OMG (Object Management Group) in 1979. It also supply common standard models for developer and makes development process easy [3-4]. Booch has introduced the UML user guide and the Object-Oriented analysis and design with applications. The key benefit of UML provides security developers standardized methodologies for visualizing security attacks that are present in security networks. With the help of Class Model and Sequence Diagrams, it can be designed the models to help increase security which is the main of present paper.

Network has become an integral part of professional users and they can share knowledge in a faster way. There are many network applications which are not secured. The basics of the network security are prevention, detection and response. Primary goal of computer and network security is the protection of the information [5-6] as given below:

Information Security = Confidential + Integrity +
Availability + Authentication.

This paper is organized into four sections. Section I depicts about the introduction of Internet Protocol and UML modeling language. In Section II, describes the literature about the security features. In Section III, describes technique in the form of RSA implementation on the IP address is described with the help of UML class model. A small but an effective Class model is proposed and implementation of RSA algorithm on the IP address is represented in the form table. Al last, section IV conclude the research work.

II. RELATED WORK

From last two three decays decade, a lot of research work is available in literature for network security but limited on IP address security and till today there is no strong algorithm is available which can secure IP address. Network security can get several times data as much as common security products because of its comprehensive security services. It is becoming more and more crucial as the volume of data being exchanged on the Internet. When people use the internet, then they want confidentiality and integrity. In [7], authors implement the security in a Wireless Sensor Network (WSN), whose wireless sensor nodes tend to be exposed by enemies. UML describes and analyzes the current attacks and counter measures. Author "Timing" has emphasized on knowledge of security protocols, design and analysis [8].

A framework with multilevel specialty techniques supported is reported in the paper which can make student deeply understand both theory and practical on network security protocols. In [9], authors introduced about the architecture of network security and security threats with some security services. In [10], the network security management system processes in a mass data with low efficiency and Accuracy are described. The experiment identified the real attacks from a large number of security events with a good performance, so that the information can be refined and the requirements of new security situations will be met. In this paper, authors implemented single-key encryption algorithm and a protocol which demonstrates the communication based on IP6.

III. PROPOSED UML CLASS MODEL FOR IP ADDRESS SECURITY

When any user works on internet then he wants security to be send the information and shared data with others. On internet every user have unique IP address for correspondence. Let us consider a sender has computer system having the IP address 192.168.109.145 through which their user is sending the data on the receiver's system as shown in the UML class model represented in Figure 1. Then this IP address is encrypted and decrypted by using the RSA algorithm. RSA is one of the first crypto systems which is widely used for secured data correspondence.

When it receive at the receiving end, if the sender IP address and receiver IP address are same then it is secured to receive at the receiving end, which is represent through a table and UML Class diagram. RSA used two keys public key and private key. The public key can be viewed by all people and is used for encryption message. This message can be decrypted in a limited time by using the private key. This key is generated by using the RSA algorithm perform as per following four steps:

1. Let us consider two prime numbers p and q;
2. Compute n=p*q,
3. Compute $\Phi(n) = (p-1)*(q-1) = n - (p = q - 1)$;

4. Compute decryption key d such that gcd(d, $\Phi(n)$)=1
   and d should be prime number;
5. Compute encryption key e such that ed mod($\Phi(n)$)=1.

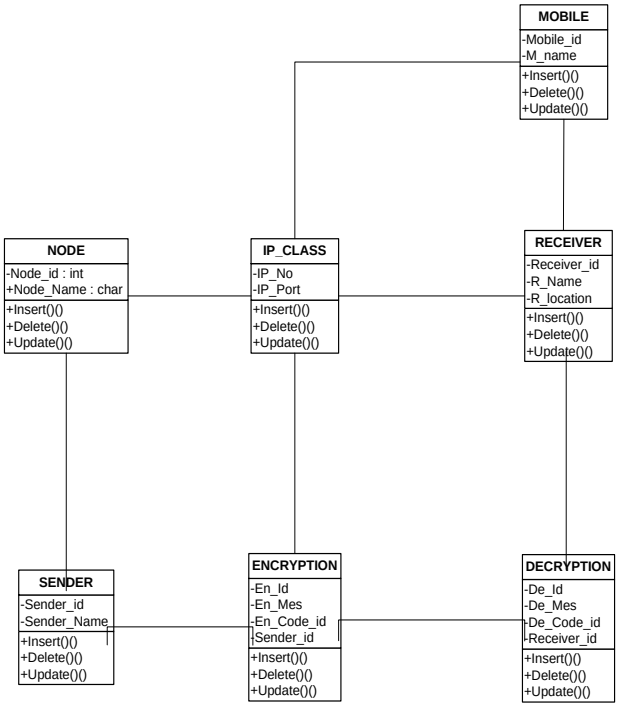

Figure 1. UML Class Model for IP Security

In the reference of above, let us consider p=3 and q=7, then n=21 and Φ(n)=2x6=12 and as per above algorithm, we obtained the encryption and decryption keys as 17 and 5, respectively which are prime numbers. The computations of above algorithm are shown in the following table. In the table a IP address for the computer system separated by the decimal dots 192.168.109.145 which is at the sender end and data is transferred on the mobile system. The encryption of the above IP is shown below and IP address is treated as the cipher text controlled with the numbers ranging from 0 to 255. The numerical computations at the receiver end known as decryption is also shown in the table and it is observed that if the data is passes from one computer system having the above said IP and follows the RSA algorithm then it can be rightly received at the destination end i.e. on the mobile system.

TABLE 1. RSA IMPLEMENTATION ON IP ADDRESS

IP No. (P)	$P^{e=17}$	$Q=P^e \bmod (n=21)$	$Q^{d=5}$	$P= Q^d \bmod (n)$
1	1	1	1	1
9	16677181699666569	18	1889568	9
2	131072	11	161051	2
1	1	1	1	1
6	16926659444736	6	7776	6
8	2251799813685248	8	32768	8
1	1	1	1	1
0	0	0	0	0
9	16677181699666569	18	1889568	9
1	1	1	1	1
4	17179869184	16	1048576	4
5	762939453125	17	1419857	5

IV. CONCLUDING REMARKS

Every user wants to used the internet on secured network. There is a lot of security features to secured the information. With the RSA algorithm, crypto-system is used to encrypt and decrypt the IP address to provide the safe Internet security features to the users. From the above work, it is concluded that one should follow the strong security algorithm when transmitted important information in the form of text, audio, video and Numerical Scientific data from one computer system to the other computer system connected through the network.

FUTURE SCOPE

Today hacking is the major problem with the user. When any user works on internet, then he is in Techno Secure Phobia. There are various grounds of security problem. Above model is used to secure IP address of the sender. Network security, Data security, IP security etc can be used as a module for security. Efficiency and complexity of the IP addresses can be measured, therefore, the presented work can be extended in this direction.

REFERENCES

[1] Ralph Becker, " IP Address Subnet Tutorial", (1999).
[2] G., Booch, J.Rumbaugh, and I Jacobson, "The Unified Modelling Language User Guide*", A*ddison-Wesley, Reading, MA, (1999).
[3] OMG, "Unified Modeling Language Specification", Version 1.3. June 1999. (http : // www.rational.com/media/uml/post.pdf) (1999).
[4] OMG, "Unified Modeling Language Specification", Available Online Via www.omg.org (2007).
[5] John E. Canavan , "Fundamentals of Network Security", (2000).
[6] Mathew T. J., "A New Packet Cipher To Secure IP Based Communications", IEEE (2009).
[7] Sunghyuck, Hong, and Sunho, Lim, "Analysis of Attack Models via UML in WSN: A Survey Study, IEEE (2010).
[8] Tieming Chen, "A Compositive Education Scenario for Network Security Protocols", Interantional Workshop on Education Technology and Computer Science (2010).
[9] Yishan Gong, Guanghong Yue and Quansheng Xu," Network Security and Safety Precautions", Second International Conference on Future Networks (2010).
[10] Lin Li and De-bao Xiao, "Research on the Network Security Management Based on Data Mining", International Conference on Advanced Computer Theory and Engineering (2010).

