Security Authorization for MAC Address under Distributed Environment

Kenam Verma
Indian Space Research Organisation
Antariksh Bhavan, New BEL Road, Bangalore-560231, INDIA

Rashmi Singh
Department of Computer Science
B. B. Ambedkar University
Lucknow (U.P.) 226025, INDIA

Vipin Saxena
Department of Computer Science
B. B. Ambedkar University
Lucknow (U.P.) 226025, INDIA

ABSTRACT
Arrangement of autonomous computer systems is one of the major issues in the distributed computing system. Each machine has its own unique Media Control Access (MAC) address. When the machine is connected across the globe on the Wide Area Network (WAN), intruders can be easily caught by the MAC address of the machine. If one transmits the confidential information from one device to another device then it is very important for safe delivery of the information with secure transmission of MAC address, so that intruders could not break the MAC address. In the present work, an approach for secure transmission of information along with the MAC address is depicted with well known Rivest, Shamir and Adleman (RSA) algorithm of the security system. The algorithm is tested on different MAC addresses of different machines through the object-oriented programming JAVA language. Before implementation, Unified Modeling Language (UML) approach is used to build a cryptosystem model.

Keywords
Distributed Computing, Media Control Access, Wide Area Network, Unified Modeling Language, Cryptosystem.

1. INTRODUCTION
A distributed computing system is a system which has made our communication a lot of easier. It combines various devices into one, which lessens the complications involved in a network. This system consists of wearable and hand-held devices which are portable too for example our mobile phones can also be connected across the globe by the use of distributed computing system. They can be either wire-based or wireless. Now, sharing is very easier, a person sitting in London can easily communicate with the Indians. It increases the performance as well as computing can be done at the remote location. LAN (Local Area Network) and WAN (Wide Area Network) are the perfect examples of such type of the system. But with the easiness also come difficulties and that involves whether the sharing is being done securely or not. A distributed computing system is shown below in figure 1.

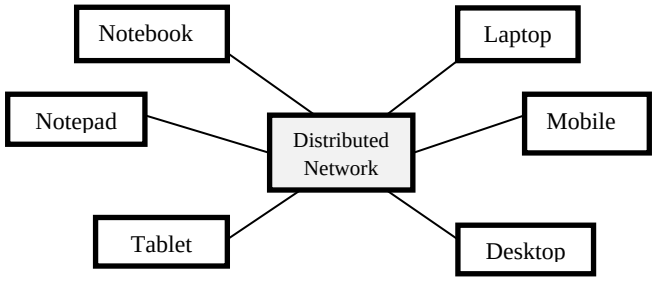

Fig.1. A Distributed Computing System

MAC addresses are also known as the physical or hardware addresses. Other names are Ethernet address or the NIC address. It stands for Media Access Control which are unique addresses provided to a device for its identification. MAC addresses are made up of hexadecimal numbers (0-9, A-F). These are used in MAC sub layer of the Data Link Layer of the OSI Reference Model. There are various notations to represent a MAC Address. The EUI -64 which is almost the same as MAC-48 notation is widely used which represents the address as six groups of 2 hexadecimal numbers separated by hyphens(-) or colons(:) in transmission order. For example, 97:45:AC:FB:01:43 or its equivalent, 97-45-AC-FB-01-43.It's a 48-bit address. Hence, there are (2^48) possible MAC addresses.

A communication is made possible only because of MAC addresses. When data is being transferred from the sender device to the receiver device, there are possibilities that it doesn't reach its destination. It might be hacked on route. So, it is important that the MAC address is perfectly matched before continuing the process of sharing. Usually in many attacks, a best example of this is the MAN in the middle attack, a MAC address can be known such that the sender thinks that the data will reach where it is destined to but the attacker gets all the data. Hence, there is a need of the hour to encrypt the MAC address so that no attacker can have the device's MAC address. The data gets into the receiver's device safely. Encryption converts the readable plain text into the unreadable cipher text. This cipher text gets transferred which is unreadable even if it gets hacked. The cipher text can be decrypted into the plain text by the private key easily. In the present work, UML stands for Unified Modeling Language. It is a way of showing graphically all the processes for the better visualization. A sender is one who sends data for effective communication to the receiver one who receives the data. Server is a medium which connects the two. So mainly, the communication can take place in three ways. First of them is, the data takes the shortest route through the server and reaches the receiver. Secondly the data through the sender gets encrypted first and then gets transferred in this way and is decrypted by the receiver. Third is the longest path, the sender sends the data to the server which encrypts the data and decrypts the data and sends it to the receiver. These three methods are represented in the UML Class model below.

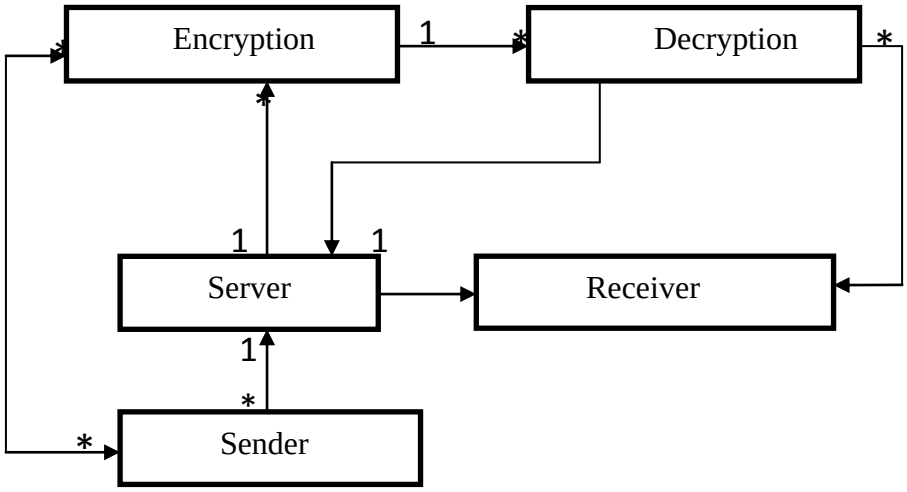

Fig.2.UML Class Representation

2. REVIEW OF WORK

Let us review important references related to the present work. Rivest et al. [1] have introduced an algorithm which is based on the prime numbers for the security of the digital signatures. Diffie and Hellman [2] discussed how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems. Tanenbaum [3] has defined the merging of computers and communications which have a profound influence on the way computer systems are organized. Milenkovic [4] emphasized on synthesis by exploring relationships among different parts of operating systems and demonstrating how they are combined to form complete systems. In a research report, Kaya Koc. [5] emphasized upon the underlying Mathematics, algorithms, and their running time analyses. OMG (Object Management Group) [6] shows the Object Management Architecture (OMA) which embodies the OMG's vision for the component software environment. OMG [7] throws the light on the UML reference model. Pointcheval and Stern [8] have exclusively focused on signatures, mainly for the security purposes. Stallings [9] covers important network security tools and applications. Krishnamurthyet et al. [10] have implemented a multi-prime 1024-bit RSA signing operation on TI TMS320C6201 DSP processor with the new reduction method. Booch et al. [11] provides the practical guidance on the analysis and design of object- oriented system. On the basis of review of literature, it is observed that MAC address are not secured through JAVA programming language, hence the present work is an attempt in this direction.

3. RSA ALGORITHM

RSA is an asymmetric encryption method used for secure data transmission. It is developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 and hence, its name as RSA. It works upon two prime numbers (usually large), namely p and q which are chosen in such a way that they are not equal. An encryption key which is a public, e helps in producing the cipher text by the formula : c=(p^e) mod m, where m= (p-1)*(q-1) and e is co-prime to m, d is the private key to be computed. A sample code of JAVA programming is given below:

```
staticBigIntegerd;

        //encryption
        privatestaticBigInteger encrypt(int
a)
        {
            // create printstream object
        PrintStreamps =
newPrintStream(System.out);
        BigInteger a1 =
BigInteger.valueOf(a);
        BigInteger c=a1.modPow(e, n);

        // printf this ciphertext
        ps.printf("The cipher text for %d is
%d  ", a,c);
            //flush the stream
        ps.flush();

            return c;
        }
        //decryption
        privatestaticchar
decrypt(BigInteger a)
        {
            BigInteger p=a.modPow(d,
n);
            //calculating the plain text
after decryption
            int p1=p.intValue();
```

```
System.out.println(p1);
charch=(char)p1;
returnch;
}
publicstaticvoid main(String args[]){
Scanner scanner = new Scanner(System.in);
System.out.println("Please enter the Mac Address");
String text = scanner.next();
System.out.println("Plain text before encryption is : "+ text);
BigInteger [] data = newBigInteger [20];
char[] plain = newchar[20];
int i;
//checking whether e and m are co-prime or not
while (m.gcd(e).intValue() > 1 ) {
e = e.add( newBigInteger( "2" ));
}
d = e.modInverse(m);
System.out.println("The value of d is \n " +d);
System.out.println("The value of e is \n " +e);
for(i=0;i<text.length();i++)
{
if(text.charAt(i)!=':'||text.charAt(i)!='')
data[i]= encrypt((int)text.charAt(i));
else
data[i]=encrypt(186);
}
for (i=0;i<17;i++)
{
plain[i]=decrypt(data[i]);
}
String pt=new String(plain);
System.out.println("\n Plain text after the decryption is : "+pt);
}
}
```

The output of the code is given below in tabular form.

Plain text before encryption is: 23:45:67:AC:BD:EF

p=17, q=11, d=23, e=7

4. RESULTS AND DISCUSSION

In this section, we show the description of steps which are included in this algorithm. First we calculated the value of n i.e. p*q =187 and now find (p^e) mod(n)=17^7 mod 187=> 118 which is the value of c i.e. cipher text which is not the original message so receiver decrypt this using private key d. Now we put the value of c i.e. 118, d=23and n=187 in (c^d) mod (n)=p and find the value of p i.e. 50 which is ASCII value of 2 and 2 is the original message. This procedure continues for each bit and gets the original message. The following table shows all bits conversion using algorithm.

Plain text(p)	**ASCII value(p)**	**(P^e)mod(n)=c**	**(c^d)mod(n)=p**	**Plain text**
2	50	118	50	2
3	51	17	51	3
4	52	35	52	4
5	53	26	53	5
6	54	164	54	6
7	55	132	55	7
A	65	142	65	A
C	67	67	67	C

B	66	110	66	B
D	68	51	68	D
E	69	86	69	E
F	70	60	70	F

```
Plain text after the decryption is:
23:45:67:AC:BD:EF

In such a manner
```

5. CONCLUDING REMARKS

In the present work, an implementation of the RSA algorithm on the MAC for secure transmission information from one device to another device is presented. Along with the data secure MAC address is also transmitted for representing the sender device. A block diagram for encryption and decryption is also presented through the UML class model which has been implemented in the JAVA programming language. The presented work can also be further upgraded for secure transmission of the text, audio and video data also. Till today, breaking of RSA is not recorded in the literature as in the computation based on prime numbers becomes too complex and very difficult to break RSA algorithm that's why it is widely used for securing the digital signature.

6. REFERENCES

[1] R.L.Rivest, A. Shamir, and L.M.Adleman.(1978). "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, volume 21, pages 120-126, February.

[2] W.Diffie and M. Hellman. (1978). "New Directions in Cryptography". *IEEE transactions on Information Theory*.IT-22.472-492.

[3] Andrew S. Tanenbaum.(1980) "Computer Networks" , Fourth Edition, 2003.

[4] Milan Milenkovic.(1987). "Operating System: Concepts and Design", Second Edition, 1992.

[5] Cetin Kaya Koc. (1994). *High speed RSA implementation*, RSA Laboratories, CA.

[6] OMG (Object Management Group): Object Management Architecture Reference Model. (1995).

[7] OMG (Object Management Group): Unified Modeling Language (UML) Reference Model. (1995).

[8] David Pointcheval and Jacques Stern. (1996). Security proofs for signature schemes, *EUROCRYPT'96*, Zaragoza, Spain.

[9] W.Stallings. (1998). "Cryptography and Network Security", Third Edition, 2006.

[10] Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang. (2002). An efficient implementation of multi-prime RSA on DSP processor, University of Texas, Texas, USA.

[11] Grady Booch, Robert A. Maksimchuk,Michael W. Engle ,Bobbi J. Young, Jim Conallen, Kelli A. Houston."Object-Oriented Analysis and Design with Applications ", Third Edition, 2007.