IMPLEMENTING DOUBLE SECURITY USING IP AND KEY ENCRYPTION IN DATA TRANSFER

Himanshu[1], Gaurav Pathak[2], Nidhi Sharma[3]
[1]M. Tech scholar, [2,3]Associate Professor
[1,2,3]Computer Science and Engg., [1,2]NIET NIMS University, Jaipur, Rajasthan, India.

Abstract: In the case of the Network, the data is required to be transferred from one destination to another. And in this transfer it is required to address the node using the IP address. As now almost all networks are subject to the hacker’s risk, so proper security is always desired. In our paper , we have proposed a secure algorithm which performs the encryption of IP and also encrypt the key. The data send is also encrypted and at the receiving end the decryption of IP takes place and only the node which decrypt IP and matches its actual IP with it will able to decrypt the encrypted message.

Keywords: Security; Network Security ,Double Security, IP Encryption , etc…

I. INTRODUCTION

The current internetworking protocol [11], IPv4, over the long haul will be not sufficiently capable sponsorship additional hubs or the necessities of new applications. IPv6 is another framework tradition that segments upgraded adaptability and controlling, security, effortlessness of-outline, and higher execution appeared differently in relation to IPv4. Tragically, IPv6 is opposite with IPv4 and to use the new tradition will oblige changes to the item in each sorted out contraption. IPv4 systems, in any case, are ubiquitous and are not going to leave "overnight" as the IPv6 structures are come in. Subsequently, it is critical to make move frameworks that engage applications to continue working while the hosts and frameworks are being upgraded. One proposed procedure is to unravel IP headers as they blend of IPv4 and IPv6 frameworks [3]. The need of header elucidation is to remain clear to applications and the framework. In this paper we show two assortments of IPv6/IPv4 interpreters that address these inconveniences. The fundamental assortment uses remarkable IPv6 addresses, as proposed in [4], to easily translate divides for all applications. Tragically, these exceptional IPv6 addresses similarly require IPv6 changes to contain phenomenal courses to them, which is believed to be a frightful idea since it makes more state for the change to keep up [4]. The second assortment keeps up an express mapping among IPv4 and IPv6 addresses, and is in like manner prepared to use standard IPv6 addresses that don't require any unprecedented treatment by IPv6 switches. Its drawback is that IP-addresses embedded in a couple of utilizations' data stream, for instance, FTP, must be overhauled additionally for the elucidation to get directly to the point. We have developed an IPv6/IPv4 framework area and tradition interpreter as a device driver running in the Windows NT working structure [15]. Our test surroundings includes the interpreter as a door among IPv6 and IPv4 has related with discrete Ethernet segments, and it realizes little execution overhead. Between several IPv6 and IPv4 hubs bestowing by methods for the interpreter, we have measured TCP information exchange limit of 7210 Kbytes/second and roundtrip package latencies of 424 microseconds over 100Mbit/second Ethernet joins. Our attempts begun with an execution of the IPv6 tradition for the SPIN [13] extensible working system, which enables the quick prototyping of part developments. In the wake of completing the fundamental IPv6 utilization we related our structure to the 6Bone [12]. We were enthusiastic about getting to organizations using IPv6, yet instantly found that there were only a few has (around 250) open by methods for the 6Bone with even less IPv6 neighborhood organizations to talk with. Hence, we built an IPv6/IPv4 interpreter to engage IPv6 structures to get to the IPv4 systems and organizations, and the a different way.

There are two essential circumstances where framework area and tradition elucidation are applicable:

- An IPv6 site talking with IPv4 hubs. For example, an absolutely new framework with new contraptions that all support IPv6 may now and again need to talk with some IPv4 hubs out on the Internet.
- An IPv4 site talking with IPv6 hubs. For example, refreshing an IPv4 site to IPv6 on a center by-center introduce requires that fundamental organizations, for instance, web, record, and print organizations are accessible from both IPv6 and IPv4 hubs.

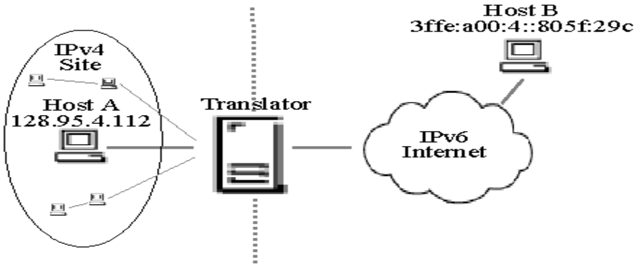


Fig..1 Translator for an IPv6 site

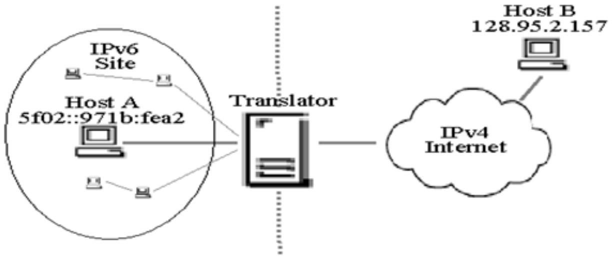
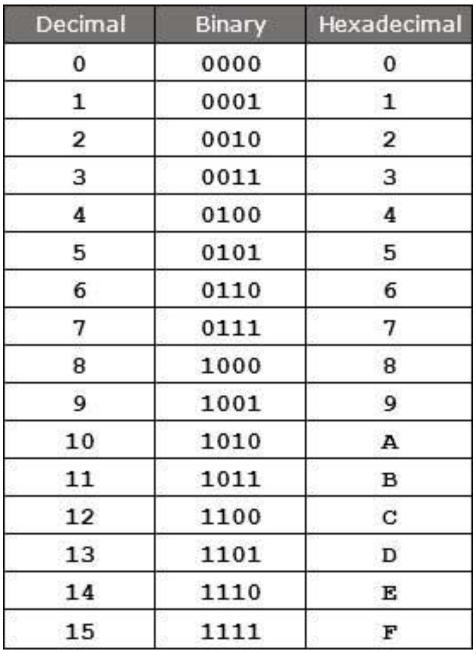


Fig.2. Translator For An Ipv4 Site.

II. IP28V6 - ADDRESS TYPES & FORMATS

2.1. Hexadecimal Number System:

Before displaying IPv6 Address gathering, we ought to examine Hexadecimal Number System. Hexadecimal is a positional number structure that uses radix (base) of 16. To address the qualities in important association, this structure uses 0-9 pictures to address esteems from zero to nine and A-F to address esteems from ten to fifteen. Every digit in Hexadecimal can address esteems from 0 to 15.



Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Fig 3. Conversion Table

2.2 Scope of IPv6 Unicast Addresses

The degree of Link-neighborhood compelled to the segment. Remarkable Local Address are locally around the world, yet are not guided over the Internet, compelling their degree to an affiliation's breaking point. Overall Unicast areas are thoroughly exceptional and obvious. They ought to make the substance of Internet v2 tending to.

In spite of the way that IPv6 packs have started to stream, framework manufactures still tread carefully because of holding up security concerns. Here are the primary six security perils in IPv6 framework security today as voted by gogoNET people, a gathering of 95,000 framework specialists.

* Lack of IPv6 security get ready/preparing. The No.1 danger today is the nonattendance of IPv6 security learning. Wanders must put time and trade out IPv6 security get ready direct, before passing on. That or peril deal and contributing more vitality and more money on security later to plug the openings. Framework security is all the more effective as a noteworthy part of the organizing stage rather than in the wake of sending. This is not a range to keep down on. As shown by Scott Hogg, IPv6 Security maker and CTO of GTRI, "All security specialists should get some answers concerning IPv6 now since all affiliations have IPv6-skilled and enabled working systems in their environment. Powerlessness to secure the IPv6 systems look like allowing a gigantic auxiliary entry to exist."

* Security device evade by methods for unfiltered IPv6 and tunneled development. Only a nonappearance of learning is seen as a more serious risk than the security things themselves. Skillfully it's direct, security things need to do two things – see suspicious IPv6 divides apply controls when they do. However before long this is not by any stretch of the imagination possible in v4 also a circumstance that may have revolt or darken entry movement. "There are 16 special sections and move techniques – likewise upper layer tunnels like: SSH, IPv4-IPSec, SSL/TLS and even DNS," says Joe Klein, Cyber Security Subject Matter Expert for the IPv6 Forum and Expert Cyber Architect at SRA International. "The underlying stride is understanding what you're hunting down." The recurring pattern collect of security things used today, especially those changed over from v4 to v6, haven't as per normal procedure adequately created to arrange the hazard they're guaranteeing against.

* Lack of IPv6 sponsorship at ISPs and traders. Serious testing is fundamental until IPv6 security handiness and soundness are keeping pace with that of IPv4. A test framework and a test course of action for all traditions included must be prepared to test all apparatus – especially new security tech from shippers. Every framework is phenomenal and requires a remarkable test mastermind however can be found on Joe Klein's and Scott Hogg's web diaries. Additionally bewildering the issue is not having a neighborhood IPv6 relationship from your provider. A section related with your interface additionally extends security multifaceted nature and gives an opening to man-in-the-middle and difference of-organization strikes. Ask for nearby IPv6 from your upstream provider.

* Congruence of security methodologies in v4 and v6. Weak v6 security methodologies are a prompt outcome of the present lack in IPv6 security learning. Not simply do the significance of the IPv6 security procedures ought to be proportionate to that of their IPv4 accomplices yet their broadness must be more broad to fuse new vulnerabilities that didn't ought to be considered in an IPv4 homogeneous condition.

* Bugs in new code. Nearby any new code will be bugs. Likewise, for this circumstance they can be found in the code around NICS, TCP/UDP and sorting out programming libraries that don't totally support IPv6 yet. Advancements, for instance, SIP, VoIP and virtualization can moreover be feeble. Ideally bugs are a bothering, even under the slightest great conditions they can introduce new vulnerabilities in your framework. The cure, as some time as of late, is attempting. A test framework and a careful test course of action will reveal betrays all around alright to disconnect them, allow workarounds to be found or to shut down an association all things considered until they're repaired.

A few cases of how your references ought to be recorded are given toward the finish of this layout in the "References" segment, which will enable you to amass your reference list as per the right organization and text dimension.

III. PROPOSED CONCEPT

In this recommendation we have proposed an answer with a particular true objective to twofold guarantee the whole structure. With a particular ultimate objective to give the twofold security, we have encoded IP address and moreover the data. Remembering the ultimate objective to encode the IP address we have taken the key which will be of 4 characters in length. Furthermore, it will scramble the IP address by including the ASCII estimation of each character to the each of the IP part. Additionally, the key is further scramble and the last IP part will be associated in the key. By and by to disentangle the IP , the system is the recipient when sort the mixed Ip with the Key , the underlying four characters of the key are at first evacuated and after that unscramble the encoded IP by subtracting the ASCII esteems furthermore the last some portion of the new IP is facilitated with whatever is left of the characters of the mixed key. Additionally, if the match then we proceed further.

3.1 Algorithm of Encrypting IP is as per the following,

```
Step 1 : Read IP,KEY
Step 2: If Length(KEY) <> 4 then Exit by Giving Error Message
Step 3: Extract each bit of IP area disengaged by .(period)
Step 4: Now find ASCII estimations of each of the four characters
Step 5: Add the both esteems to get the mixed IP implied by EIP.
Step 6: Now last IP some portion of our real IP is removed and linked with the KEY to frame the new EKEY.
```

3.2 Algorithm of Decrypting IP is as per the following,

```
Step 1 : Read EIP,EKEY
Step 2: Extract beginning four character of EKEY and find their ASCII esteems.
Step 3: Extract each bit of EIP area confined by .(period)
Step 4: Subtract the both esteems to get the honest to goodness IP meant by IP.
Step 5: Now last IP a segment of our honest to goodness IP is isolated and differentiated and the characters after the underlying four characters in the EKEY.
Step 6: If both match then we will proceed further.
```

3.3 Scrambling the Plain Text

By and by the Message is also further mixed and for this circumstance we will take after the going with steps.

```
Step 1: Read PTEXT
Step 2: KEY presented with
Diminish KEY_128 As Byte() = {42, 1, 52, 67, 231, 13, 94, 101, 123, 6, 0, 12, 32, 91, 4, 111, 31, 70, 21, 141, 123, 142, 234, 82, 95, 129, 187, 162, 12, 55, 98, 23}
Step 3: IV introduced with
Diminish IV_128 As Byte() = {234, 12, 52, 44, 214, 222, 200, 109, 2, 98, 45, 76, 88, 53, 23, 78}
Step 4 : CTEXT which is cipher text is framed.
```

3.4 Decrypting the Plain Text

By and by the Message is furthermore decoded after the acknowledgment of IP and for this circumstance we will take after the going with steps.

```
Step 1: Read CTEXT
Step 2: KEY introduced with
Diminish KEY_128 As Byte() = {42, 1, 52, 67, 231, 13, 94, 101, 123, 6, 0, 12, 32, 91, 4, 111, 31, 70, 21, 141, 123, 142, 234, 82, 95, 129, 187, 162, 12, 55, 98, 23}
Step 3: IV introduced with
Diminish IV_128 As Byte() = {234, 12, 52, 44, 214, 222, 200, 109, 2, 98, 45, 76, 88, 53, 23, 78}
Step 4 : PTEXT which is plain text is framed.
```

Utilize the utilizing proclamation (as demonstrated in the specimen code that takes after) on the accompanying namespaces:

- System
- System.Security
- System.Security.Cryptography
- System.Text
- System.IO

With the goal that you don't need to qualify announcements from these namespaces later in your code. You should utilize these announcements before some other revelations.

```
utilizing System;
utilizing System.IO;
utilizing System.Security;
utilizing System.Security.Cryptography;
utilizing System.Runtime.InteropServices;
utilizing System.Text;
```

- Generate a puzzle key to scramble and to unscramble the data. The DESCryptoServiceProvider relies on upon a symmetric encryption computation. The symmetric encryption requires a key and a presentation vector (IV) to encode the data. To unscramble the data, you ought to have a similar key and a similar IV. You ought to similarly use a similar encryption estimation. You can make the keys by using both of the going with methods:

•Method 1 You can incite the customer for a mystery word. By then, use the watchword as the key and the IV.

•Method 2 When you make another event of the symmetric cryptographic classes, another key and IV are therefore made for the session. Use the key and IV that are delivered by the directed symmetric cryptographic classes to scramble and to unscramble the archive.

For more information about how to make and circle keys, see the Microsoft .NET Framework SDK Documentation, or see the going with Microsoft Developer Network (MSDN) Web site:

IV. CONCLUSION AND FUTURE WORK

Security is the most extreme prerequisite in each part of our life. On account of the system the security is must and there are number of algorithms and ideas are proposed keeping in mind the end goal to upgrade the security. In the comparative design we have likewise delivered the light weighted algorithm to upgrade the security component, in which we have scrambled the IP, Key and message to twofold insurance of the framework. Later on work we will attempt to execute this algorithm hard wired that we will implanted this algorithm in the system observing frameworks itself so that the further programming based usage won't be required to actualize this security

REFERENCES

[1] G.H. Forman and J. Zahorjan, "The Challanges of Mobile Computing," Computer, April 1994

[2] D.F. Bantz, "Wireless LAN Design Alternatives," IEEE Network, March/April 1994, pp. 43-53.

[3] H. Ahmadi, A. Krishna, and R. O. Lamaire, "Design

Issues in Wireless LANs," Journal of High Speed Networks, Vol. 5, 1996, pp. 87-104.

[4] T. F. La Porta, K.K. Sabnani, and R.D. Gitlin, "Challenges for Nomadic Computing: Mobility Management and Wireless Communications," Mobile Networks and Applications, Vol. 1, 1996, pp. 3-16.

[5] R. Bagrodia, W.W. Chu, L. Kleinrock, and G. Popek, "Vision, Issues, and Architecture for Nomadic Computing," IEEE Personal Communications, December 1995, pp. 14-27.

[6] K. Pahlavan, T.H. Probert, and M.E. Chase, "Trends in Local Wireless Networks," IEEE Communications Magazine, March 1995, pp. 88-95.

[7] E. Links. W. Diepstraten and V. Hayes, "Universal Wireless LANs," Byte, May 1994, pp. 99-108.

[8] B. Jabbari, et al, "Network Issues for Wireless Communications," IEEE Communications Magazine, January 1995, pp. 88-98.

[9] A.K. Salkintzis and C. Chamzas, "Mobile Packet Data Technology: An Insight into MOBITEX Architecture," IEEE Personal Communications Magazine, February 1997, pp. 10-18.

[10] R.H. Katz, "Adaptation and Mobility in Wireless Information Systems," IEEE Personal Communications, First Quarter 1994, pp. 6-17.

[11] K.C. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September/October 1994, pp. 50-63.

[12] C.A. Rypinski, "Standards Issues for Wireless Access," Business Communications Review, August 1992, pp. 40-45.

[13] G. Fay, "Wireless Data Networking," International Journal of Network Management, 8 March 1992, pp. 8-17.

[14] D.J. Goodman, "Second Generation Wireless Information Networks," IEEE Transactions on Vehicular Technology, Vol. 40, No. 2, May 1991

[15] D. Buchholz, et al, "Wireless In-Building Network Architecture and Protocols," IEEE Network Magazine, November 1991, pp. 31-38.

[16] Hayes, "Standardization Efforts for Wireless LANs," IEEE Network Magazine, November 1991, pp. 19-20.

[17] D.J. Goodman, "Cellular Packet Communication," IEEE Transactions on Communications, August 1990, pp. 1272-1280.4.