Security Model for TCP/IP Protocol Suite

M. Anand Kumar
Department of Information Technology, Karpagam University, India
anandm_ss@yahoo.co.in

Dr. S. Karthikeyan
Department of Information Technology, College of Applied Sciences Sultanate of Oman
skaarthi@gmail.com

***Abstract*—the Internet has instantly evolved into a vast global network in the growing technology. TCP/IP Protocol Suite is the basic requirement for today's Internet. Internet usage continues to increase exponentially. So network security becomes a growing problem. Even though IPv6 comes with build mechanism IPsec for security, it lacks security in Application layer of TCP/IP protocol suite. IPv6 solves most of the security breaches for IPv4 with the use of IPsec. But IPsec doesn't have any security provision in the application layer. So there is a need for security mechanism. In this paper some of the security flaws of IPv6 are identified and we present a new architecture for TCP/IP protocol suite. Our proposed architecture includes a layer called security layer, which guarantees security to Application layer using a protocol Application layer security protocol (ALSP).**

***Index Terms*— Internet, TCP/IP, Cryptography, Security, Protocol**

I. Introduction

The perception of security is traditionally connected to exigencies of defending sensitive data from illegal access. But at the moment network security is often approached from a different perception. With the growing use of the Internet infrastructure for commercial applications, the demand for Quality of service is one of the emerging paradigms in Internet and seems to be the corner stone for more and more network services [1]. An increasing number of applications need multifaceted, consistent control protocols for guaranteeing Quality of service. As an outcome the need for security in network infrastructure is stronger than ever. Internet is based on TCP/IP protocol suite. IP was not planned with security in mind. The severe security flaws of the TCP/IP protocol suite exist since the host relies on IP source address for authentication.

The existing network layer protocol in the TCP/IP protocol suite is at present IPv4 (Internet-working protocol version 4). Even though IPv4 is well designed, its security breaches make it inappropriate for the fast emerging Internet. To over come these drawbacks, IPv6 (Internet-networking protocol version 6) also known as IPng was planned which became a standard in the recent past. [1].

Internet Protocol version 6 or IPv6 is an enhanced version of the IPv4, which is a current version, and most widely used Internet Protocol. IP enables data to be sent from one workstation to another in a network and is known as a connectionless protocol since there is no continuous connection between the two communicating devices. Therefore when a message is sent by means of IP it is broken up into packets, which may travel through a number of different routes to their final destination, and on arrival at their destination they are reassembled in their original form. Each device in a network has an IP address, which is used by the IP protocol to ensure that the packets of information reach their correct destination. It holds great guarantee to become the backbone of the prospect of the Internet and offers an important improvement over IPv4 in terms of scalability, security, mobility and convergence [2]. The Internet Engineering Task Force (IETF) standardized the basic framework of the IPv6 protocol in the 1990s. But, there is still ongoing development of certain advanced aspects of the protocol [2].

The rest of the paper is presented as follows. In section II we describe the architecture of TCP/IP model followed by cryptographic algorithms in section III. We then describe the proposed architecture in section IV. In section V, we analyze the performance and finally conclude in section VI.

II. TCP/IP ARCHITECTURE OVERVIEW

The TCP/IP protocol suite, as well referred to as the Internet protocol suite, is the set of communications protocols that implements the protocol stack on which the Internet and most commercial networks run. It is named after the two most important protocols in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Internet Protocol is the foundation of the TCP/IP protocol suite, since it is the mechanism responsible for delivering datagram's The TCP/IP protocol suite—like the OSI reference model—is defined as a set of layers.

Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that are transmitted physically over the network [4]

doi:10.4304/jait.2.2.87-91

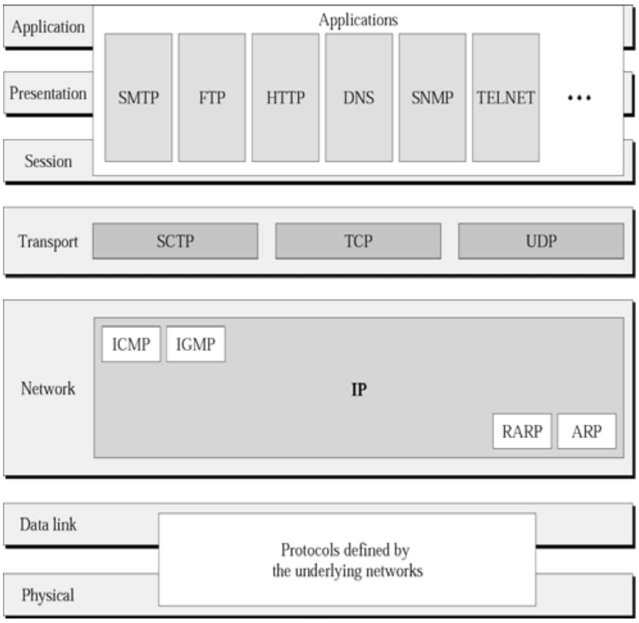

Figure 1. TCP/IP Protocol Suite Architecture [8]

A. IPv6 Security Enhancements

IPv6 security is very similar to that of IPv4 in terms of security. The process of transporting packets across different networks is similar and the upper layer protocols that are concerned with transporting actual applications are not affected. IPv4 provides IPsec support, which is optional. But in the case of IPv6, IPSec is a requirement rather than optional. Due to these reasons it is stated that IPv6 is more secure than IPv4 that will be true only in an environment with well coded applications. IPv6 is usually deployed without cryptographic protection of any kind. IPsec is an Internet security protocol integrated into layer2 that is network layer to secure the network from the unauthorized users through origin authentication, data confidentiality and data integrity. IPsec does not guarantee any security in the application layer, where more security breaches occur [3]. IPsec provides security services at the network layer by enabling a system to select required security protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more paths between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. The set of security services that IPsec can provide includes access control, connectionless integrity, and data origin authentication, rejection of replayed packets, confidentiality and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc. IPsec uses two protocols to provide traffic security services Authentication Header (AH) and Encapsulating Security Payload (ESP).IPsec implementations must support ESP and AH[3].

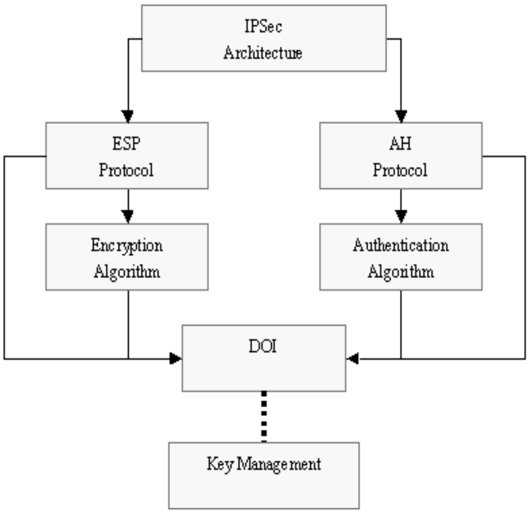

Figure 2. IPsec Architecture [9]

The IP Authentication Header offers integrity and data origin authentication, with optional anti-replay features. The Encapsulating Security Payload protocol offers the same set of services, and also offers confidentiality. Use of ESP to provide confidentiality without integrity is not recommended. When ESP is used with confidentiality enabled, there are provisions for limited traffic flow confidentiality, i.e., provisions for concealing packet length, and for facilitating efficient generation and discard of dummy packets. This capability is likely to be effective primarily in virtual private network (VPN) and overlay network contexts [4]. Both AH and ESP offer access control, enforced through the distribution of cryptographic keys and the management of traffic flows as dictated by the Security Policy Database (SPD). These protocols may be applied individually or in combination with each other to provide IPv4 and IPv6 security services. However, most security requirements can be met through the use of ESP by itself. Each protocol supports two modes of use: transport mode and tunnel mode. In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets. IPsec allows the user (or system administrator) to control the granularity at which a security service is offered. For example, one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel can be created for each TCP connection between each pair of hosts communicating across these gateways [3]. IPsec, through the SPD management paradigm, incorporates facilities for specifying: which security protocol (AH or ESP) to employ, the mode (transport or tunnel), security service options, what cryptographic algorithms to use, and in what combinations to use the specified protocols and services, and the granularity at which protection should be applied. Because most of the security services provided by IPsec require the use of cryptographic keys, IPsec relies on a separate set of mechanisms for putting these keys in place. This requires support for both manual and automated distribution of keys. It specifies a specific public-key based) for automated key management, but other automated key distribution techniques may be used. It is suggested that IPv6 is more secure than IPv4 because of the inclusion of IPSec[4]. But the case is not true in most of the occasions. In the next section we are going to discuss some of the security flaws of the latest versions.

B. IPv6 Security Issues

It is observed that the use of IPsec for securing valuable information should be avoided until IPSec is improved. Even though IPv6 provide better security for the network layer, there exists some of the security issues such as intrusion and Denial of service is possible. Here are some of the issues related to IPv6:

- Intrusion: IPv6's advanced network discovery lets the end user to select the path for their packets; this provides the way for attackers to drill down and get more information about the network and also provide the way to interact with equipment not in direct sight.
- Filtering device bypass: Filtering devices such as firewalls were not designed for IPv6. Such firewalls in place, an attacker could hide traffic or a payload using Route Header 0.
- Denial-of-service: DOS attacks can occur when IPv6 packets are sent back and forth through the same link until they overwhelm bandwidth. And you know what can happen after that -- not just the service disruption itself, but other attacks that are masked by the DOS.
- Anycast: Any cast works by announcing the same IP at many places on Internet so that each box can go to the nearest one. So makes the IPV6 security more badly.

Along with these problems, IPSec don't have any security mechanism for the applications that run on application layer of TCP/IP model, which is a major concern for the researchers. Either IPSec should be modified to improve application layer security or TCP/IP model should include a layer for security for application layer.

III. CRYPTOGRAPHIC ALGORITHMS

Cryptography algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. Numerous encryption algorithms are extensively available and can be categorized into symmetric and asymmetric key. Some of the common algorithms are RE 2, DES, 3DES, RC6, Blow fish, Elgamal and AES. Among these algorithms Blowfish and Elgamal are taken for the analysis that can be used for the proposed architecture.

A. Blowfish

Blowfish [7] is a variable length key, 64-bit block cipher. The algorithm consists of two parts: A key–expansion part and a data encryption part. Key expansion part converts a key of at most 448 bits into several sub key arrays totally 4168 bytes. Blowfish uses a large number of sub keys. These keys must be precomputed before any data encryption or decryption. The key array also called p-array consists of 18 32 bit sub keys: p1,p2,….,p18. There are four 32 bit s-boxes with 256 entries each. S1, 0, S1, 1… S1, 255; S2, 0, S2, 1... S2, 255; S3, 0, S3, 1....., S3, 255; S4, 0, S4, 1… S4, 255; Data encryption occurs via a 16 round Feistel network [reference]. Each round consists of a key dependent permutation, a key and a data dependent substitution. All operations are EX-Ors and additions on 32 bit words [7].

Algorithm .1 (Encryption)

```
1. The input is a 64 bit data element, X.
2. Divide X into two 32 bit halves: XL,XR.
3. then for i=1 to 16:
4. XL=XL XOR Pi
5. XR=F(XL) XOR XR
6. swap XL and XR
7. swap XL and XR again to under the last swap
   After 16 round.
8. then XR=XR XOR P17 and XL=XL XOR P18
9. Recombine XL and XR to get cipher text.
```

Decryption for Blowfish is relatively straightforward. Ironically, decryption works in the same algorithmic direction as encryption beginning with the cipher text as input. How ever as expected, the sub keys are used in reverse order.

B. Elgamal.

The Elgamal encryption system is an asymmetric key encryption algorithm for public key cryptography that is based on the Diffie Hellman key agreement. Elgamal encryption consists of three components: the key generator, the encryption algorithm and the decryption algorithm.

Algorithm 2 (Key Generation)

```
1. Choose large prime p.
2. Choose primitive elements α Є Z*p .
3. Choose secret key α Є {2,3,….,p-2}.
4. Compute β = α α mod p.
5. Public Key: Kpub = (p, α, β).
6. Private Key: Kpr = (a).
```

Algorithm 3 (Encryption)

```
1. Choose k Є {2,3,…,p-2}.
2. Y1 = αk mod p.
3. Y2 = x. βk mod p.
4. Encryption: = eKpub(x,k)=(Y1,Y2).
```

Algorithm 4 (Decryption)

```
1. X=dKpr(Y1,Y2 ) = Y2 (Y1α)-1 mod p.
```

These two algorithms are taken for the consideration based on the security and performance metrics. Both these algorithms are used in our proposed protocol without any modification. Transferring files between two systems through the proposed ALSP Protocol tests these two algorithms.

IV. Proposed System

The existing TCP Protocol suite architecture doesn't have any specific security mechanism for application layer, which is major setback. In the network layer of TCP/IP Protocol suite, IPSec provides the security mechanisms by which a system can select required protocols as well allow them to identify the algorithms that are used for the security services and to select cryptographic mechanism that suits their environments. IPSec can be used to protect communication lines between a pair of security gateways or between a security gateway and a host. The services that are provided by the IPSec include authentication, connectionless integrity, access control and confidentiality. The security services provided by IPSec can also be used by other layer protocols such as TCP, UDP, ICMP, BGP, etc

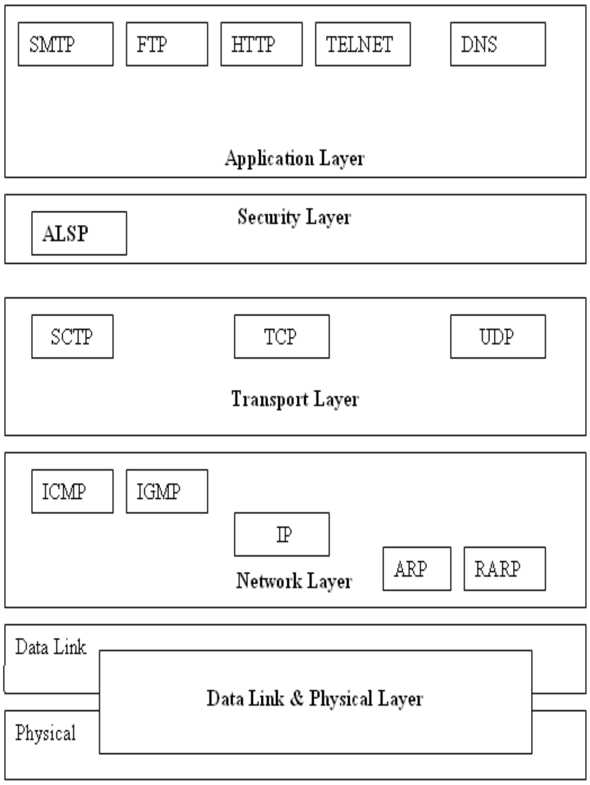

Figure 3. Proposed Protocol Suite architecture

In the proposed system, we had included a layer called security layer between transport layer and the application layer. In the security layer we had proposed security protocol called Application Layer Security Protocol (ALSP). It was designed in such a way that it provides a tight security for applications in the application layer. Cryptographic algorithms are included in the proposed protocol, such as way that TCP/IP Provide maximum security for the application layer.

V. Performance Evaluation

Performance is the vital part of the TCP/IP Protocol suite. Several performance metrics are used to evaluate the performance of the encryption algorithms such as Encryption time, Decryption time, CPU process time, and CPU clock cycles and Battery. To demonstrate the performance for the proposed architecture, a series of simulation runs are performed on a variety of set of data. Table 1 shows the data that are collected after the first run of simulation. The algorithm is executed as five rounds each with different number of files.

TABLE I DATASET FROM SIMULATION

Round	No of Files	Original Architecture	ALSP Architecture
1	1	300 ms	420 ms
2	3	800 ms	925 ms
3	5	1750 ms	2500 ms
4	8	820 ms	900 ms
5	10	2200 ms	2300 ms

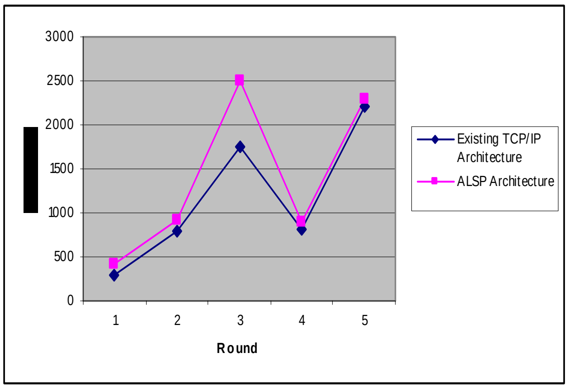

Figure 4. Performance analysis

From the analysis, it shows that the proposed architecture has poor performance when compared to the existing TCP/IP architecture. It also shows that the execution time of encryption algorithm is very high which a major reason for the lack of performance is. With the results from Figure 1, an obvious approach is required to enhance the performance of the proposed architecture. The simulation shows that if the execution time of the encryption algorithm is reduced then the performance of the proposed system can be increased. In the proposed architecture, two encryption algorithms namely blowfish and elgamal were used. In this blowfish is taken for consideration. The blowfish algorithm is evaluated in such a way to reduce the execution time. In the near future we would modify the blowfish algorithm to reduce the execution time.

VI. Conclusion

This paper has outlined several security problems of IPv6. It also outlines new ideas to design efficient security mechanism for the TCP/IP Protocol suite. With minor changes in the existing model, high level of security can be obtained. Some of the potential applications include applications in the application layer such as file transfer, email, telnet etc. In the future a complete new architecture for TCP/IP Protocol will be proposed in such a way that it provides tight security with the minor overhead of the existing model based on this ALSP architecture.

Acknowledgment

We express our heartfelt thanks to my doctorate guide, Dr. S. Karthikeyan, Asst Professor, College of Applied Sciences, Oman who offered his whole hearted guidance and invaluable suggestions throughout the preparation of this paper. I would like to express my sincere thanks to Mr. K. Appathurai, Asst.Professor and Head, Department of Information Technology for his valuable support in preparing this paper. Above all I must and do thank God Almighty from the depth of my heart for the being with me at each and every stage assuring hope, confidence and courage to get the task accomplished in time.

References

[1]. Francesco Palmieri and Ugo Fiore. “Enhanced security strategies for MPLS signaling”, Journal of Networks, 2(5), 2007

[2]. Caicedo, C.E, Joshi, J.B.D, Tuladhar. S.R. 2009. IPv6 Security Challenges. IEEE Journal of Computers, 42(2), 36-42.

[3]. Yongguang Zhang, Malibu.C.A. 2004. A multilayer IP security protocol for TCP Performance enhancement in wireless networks. IEEE Journal on Selected areas in communication, 22(4), 767-776.

[4]. http://www.ietf.nl/internet-drafts/draft-ietf-ipsec-rfc2401bis-01.txt

[5]. Douligeris, C, Douligeris, C, Serpanos, D. Serpanos, D. 2007.IP Security (IPSec) . IEEE Book: Network Security: Current Status and Future Directions, 65 – 82

[6]. Mohammad Al-Jarrah, Abdel-Karim R. Tamimi. 2007. A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement. IEEE Conference in Innovations in Information Technology,1-5

[7]. Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E,” Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect”, International Journal of Computer Science and Network Security, 8(3), 2008

[8]. Behrouz A. Forouzan. TCP/IP Protocol Suite. 3rd Edition. New Delhi: Tata McGraw Hill Publication. 2003

[9]. http://www.javvin.com/protocolIPsec.html

[10]. Bradner, S., “The End-to-End Security,” IEEE Security & Privacy, vol., no.pp., 76-79, Mar.-Apr. 2006

[11]. Skarmeta, A.F.G. Perez, G.M. Reverte, S.C. Millan.2003. PKI services for IPv6”, IEEE Internet Computing, 7(3), 36-42.

[12]. Hiromi, R.; Yoshifuji, H., “Problems on IPv4-IPv6 network transition,” Proceedings of the International Symposium on Applications and the Internet Workshop, Saint 2005,

[13]. Heng Yin Haining Wang.2007. Building an Application-Aware IPsec Policy System, IEEE/ACM Transactions on Networking 15(6), 1502 – 1513

[14]. Downnard I.2003. Public-key cryptography extensions into Kerberos, IEEE Potentials, 21(5), 30 – 34.

[15]. S. Kent. 1989. Comments on security problems in the TCP/IP protocol suite, ACM SIGCOMM Computer Communication Review,19(3),10-19.

[16]. L.Colitti, G. D. Battista, and M. Patrignani: IPv6-in-IPv4 tunnel discovery: methods and experimental results. IEEE Transactions on Network and Service Management, vol. 1, no.1. April. 2004

[17]. M.Mathis, Reflections on the TCP Macroscopic Model, Computer Communication Review, volume 39, number 1, Jan 2009

M. Anand Kumar has completed M.Sc and M.Phil in computer science and currently working as a Lecturer in Karpagam University having six years experience in teaching. He is pursuing PhD in computer Science under the guidance of Dr. S. Karthikeyan, who is working as Asst. Professor in Department of Information Technology College of Applied Sciences Sultanate of Oman. His area of research includes network security and information security. He has presented fifteen papers in national conferences and four papers in international conferences. He has published three papers in international journals.

Dr.S.Karthikeyan presently working as Assistant Professor, College of Applied Sciences, Oman and previously he was a Senior Lecturer at Caledonian College of Engineering, Oman. He was a Professor & Director at Karpagam University, School of Computer Science and Applications, Coimbatore. He has total of 14 years of teaching and research experience. Dr.Karthikeyan completed his PhD at Alagappa University, Karaikudi, India in the area of Network Security, Computer Science and Engineering by Feb 2008. He has 32 research papers and guiding 11 PhD research scholars from various universities in India and he has also guided 19 M.Phil students. He is Chief and guest editor of various national and international journals. He has chaired many conference sessions and served as Technical Committee member of various boards at various colleges, universities and conferences.