ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A New Security Architecture for TCP/IP Protocol Suite

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

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

Abstract: With the rapid growth and usage of Internet, network security becomes a major issue in the field of research. TCP and IP are the two protocols, which is basis for today's Internet. IPv4 is the Internet protocol that is replaced with IPv6, which comes with the build mechanism called IPsec for security. But it lacks security in the application layer of TCP/IP Protocol suite. So there is a need for security mechanism especially for applications in the application layer. This paper identifies some of the security problems related to IPv6 and presents 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). Simulation results show that the proposed architecture provides strict security with minimum overhead in the terms of processing.

Key words: Internet, TCP/IP, Cryptography, and Security, Protocol

I. INTRODUCTION

Internet has instantly developed into a vast global network that is used by thousand of users and controlled by different administrative entities Network security is mainly concerned with protecting sensitive data from unauthorized users and applications. But in the current scenario securing data is often approached from different viewpoint. With the increasing use of Internet for business applications, there is a great demand for Quality of service. The application that is increasing day-by-day needs a consistent control protocols for providing quality of service (QOS). Because of these reasons the need for security in the Internet is stronger than ever. The current Internet infrastructure is based on the TCP/IP protocol suite in which the Internet protocol (IP) was not implemented with security in mind. So lot of security problems exists in the TCP/IP model where the host relies an IP source address for authentication. IPv4 (Internet Protocol version 4) is the current network layer protocol of TCP/IP model [1].

The Internet Protocol (IP) is a network-layer protocol that contains addressing information and control information that is used to route the packet through the network. Two versions of IP exists namely IPv4 and IPv6. IPv4 is the current version that is most widely used. It is a connectionless protocol that is mainly concerned with transmitting data from one workstation to another [2]. Each device in the network has an IP address that is used by the IP protocol to ensure that the data packets reach the correct destination. IPv4 uses only 32-bit address, which is a major setback. With the growth of Internet will not only be computers that will need to be addressed but also household appliances such as microwaves, televisions and DVD players may be next. The existing IPv4 protocol would not be suitable for this kind of technology growth. With mobile phones connecting to the Internet and becoming more networked devices, the IPv6 protocol has features such as stateless auto configuration and neighbour discovery, which assigns addresses automatically. This allows users to maintain connections when moving into new networks. Even though IPv6 overcome most of the limitations of IPv4, still further research is required especially in the field of security [3].

The rest of the paper is organized as follows. The architecture of TCP/IP Protocol is described in section 2 that is followed by cryptographic algorithm in section 3. In section 4 security flaws of IPv6 is presented. The proposed architecture is presented in section 5and the performance is evaluated in the section 6. Finally we conclude in section 7.

II TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite that is also known as Internet protocol suite is an industry standard that is designed for large networks in which network segments are interconnected by routers. It is a protocol that is basis for today's Internet. The TCP/IP protocol suite was developed earlier to that of OSI model. As a result, the layers in the TCP/IP protocol suite do not match precisely with the layers of OSI model. The TCP/IP Protocol suite comprises five layers namely physical, data link, network, transport and application. The first four layers offer the physical standards, network interfaces, internetworking and transport functions that correspond to the first four layers of the OSI model. The three topmost layers of OSI model is represented as a single layer called application layer in the TCP/IP [1].

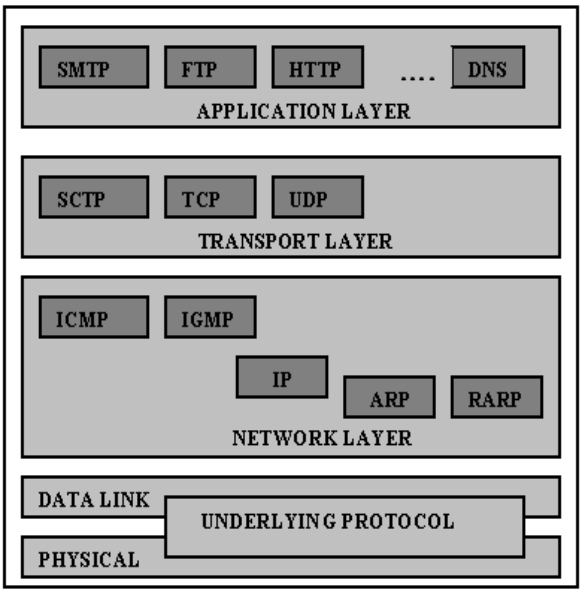

Figure 1. TCP/IP Protocol Suite

TCP/IP is a hierarchy protocol designed as interactive modules, each of which provides a specific functionality, but the modules are not necessarily independent. Where as the OSI model specifies which function belongs to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the need of the system. The term hierarchical means that each upper layer protocol is supported by one or more lower level protocols. At transport layer, TCP/IP defines three protocols: TCP, UDP, and SCTP. At network layer, the main protocol defined by TCP is IP, although there are some other protocols that support data movement in this layer [1].

III CRYPTOGRAPHY

Cryptography is a science that uses mathematical calculations to encrypt and decrypt data. It also permits the users to store sensitive information or transmit it across insecure networks. So that it cannot be read by anyone except the intended recipient. While providing privacy remains a central goal, the field has expanded to encompass many others including not just other goals of communication security such as guaranteeing integrity and authenticity of communications but also many more sophisticated and fascinating goals. Basically two types of cryptographic algorithms exist such as symmetric and asymmetric algorithms. Some of the symmetric algorithms are DES, AES, CAST – 128/256, International Data Encryption algorithm (IDEA), Rivest Ciphers (RC1 – RC6), Blowfish, Two fish, Camellia, Secure and fast encryption routine (SAFER), and SEED. Some of the asymmetric algorithms are RSA, Diffie- Hellman, Digital Signature Algorithm (DSA), Elgamal, Elliptic Curve Cryptography (ECC), Public-Key Cryptography Standards (PKCS), Cramer-Shoup, Key Exchange Algorithm (KEA), and LUC. These algorithms are analyzed to use them in the proposed architecture. From the analysis it shows that IDEA that is a symmetric cryptography is highly secure with good performance when compared to others. In this proposed architecture Blowfish algorithm is used along with Elgamal and MD5 hash algorithm [5].

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 pre computed 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].

Encryption algorithm

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.

It is a public-private encryption algorithm where each user has a public key and a corresponding private key. The public key can be used to encrypt data, but private key is used to decrypt the data. If sender publish his public key then everyone can encrypt a message using sender's public key, but only the sender can decrypt the message. Elgamal is based on the Diffie Hellman key agreement. Elgamal algorithm is analyzed in many environments. The analysis shows the strong nature of the algorithm. It is very difficult to break the key or data. Elgamal encryption is implemented by using three components namely the key generator, the encryption algorithm and the decryption algorithm.

Key generation algorithm

1. Choose large prime p.
2. Choose primitive elements $\alpha \in Z^*p$.
3. Choose secret key $\alpha \in \{2,3,….,p-2\}$.
4. Compute $\beta = \alpha^{\alpha} \bmod p$.
5. Public Key: Kpub = (p, α, β).
6. Private Key: Kpr = (a).

Encryption algorithm

1.Choose $k \in \{2,3,…,p-2\}$.
2. $Y1 = \alpha k \bmod p$.
3. $Y2 = x. \beta k \bmod p$.
4. Encryption: = eKpub(x,k)=(Y1,Y2).

Decryption algorithm

1. $X=dKpr(Y1,Y2) = Y2\ (Y1\alpha)^{-1} \bmod p$.

These two algorithms are taken for the consideration. 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.

C. *MD5 Algorithm*

The MD5 checksum for a file is a 128-bit value, something like a fingerprint of the file. There is a very small possibility of getting two identical checksums of two different files. This feature can be useful both for comparing the files and their integrity control. We begin by supposing that we have a b-bit message as input, and that we wish to find its message digest. Here b is an arbitrary nonnegative integer; b may be zero, it need not be a multiple of eight, and it may be arbitrarily large. We imagine the bits of the message written down as follows:

m_0 m_1 ... m_{b-1} (1)

The following five steps are performed to compute the message digest of the message.

1. Append Padding Bits
2. Append Length
3. Initialize MD Buffer
4. Process Message in 16-Word Blocks
5. Output

The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly. The MD5 algorithm is an extension of the MD4 message-digest algorithm.

IV PROPOSED ARCHITECTURE

In the proposed system, a layer called security layer is included 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 very high 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.

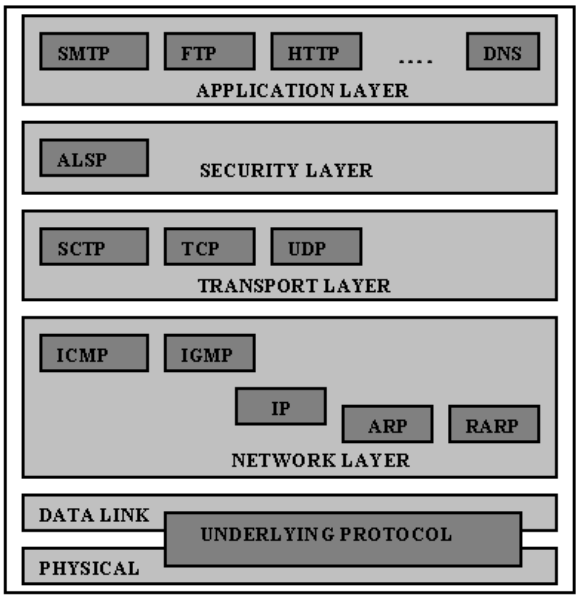

Figure 2. Proposed TCP/IP Architecture

Sender Side Algorithm

1. The data is encrypted using BF Ct = ID (Pt)
2. The keyk is Encrypted using ELG Ck= ELG (k)
3. Message digest for data using MD5 dg = MD5 (Pt)
4. Encrypt digest using ELG Cm= ELG (dg)
5. Send Ct, Ck, Cm to destination

Receiver Side Algorithm

1. The key is decrypted using ELG Dk = ELG (k) = k
2. The key k is used to decrypt text Dt=BF (Ct)= Pt
3. Message digest for data using MD5 MD = MD5 (Pt) = dg
4. Decrypt digest using ELG Pm = ELG (Cm) = dg
5. Compare dg from Step 3 and Step 4.
6. If equal data is accepted else rejected.

Where BF = Modified Blowfish algorithm Pt = Plain text
ELG = Elgamal algorithm, Ck = Cipher Key
Ct = Cipher text, dg = Message Digest

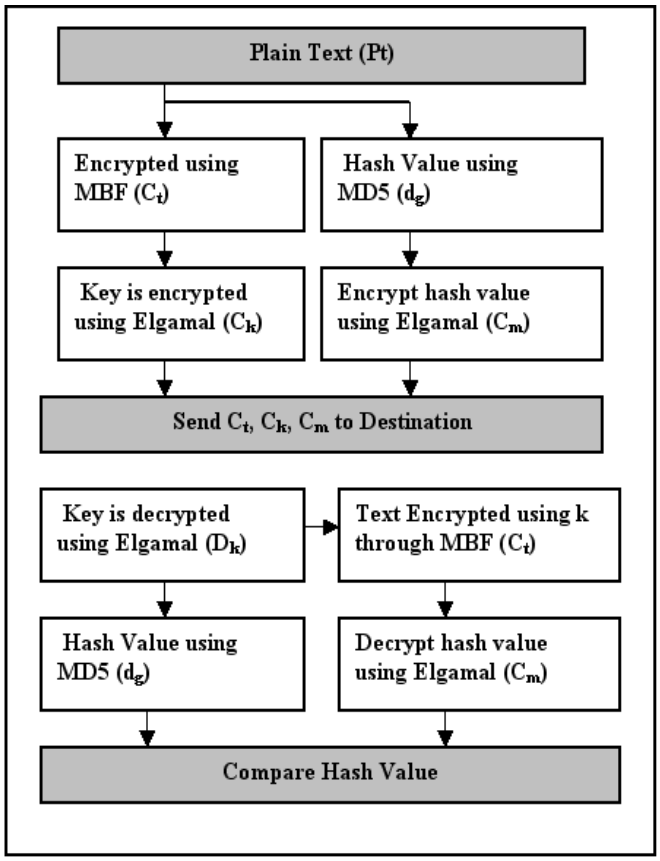

Figure 3. Proposed ALSP Architecture

The ALSP architecture uses three cryptography algorithms to provide better security. First the plain text Pt is encrypted using Blowfish encryption. The keyk that is used for encryption is further encrypted using Elgamal encryption. Then the cipher text Ct along with the cipher key Ck will be send to destination. At the same time message digest for the plain text will be calculated using MD5. Then the message digest will be encrypted using Elgamal encryption. Now Cm will be sent to destination along with Ct, Ck. At the receiver end first the key is decrypted using elgamal decryption. Next with the obtained key the Cipher text is decrypted. At the same time message digest is calculated using MD5. Then the message digest that is received from the source end is compared with the digest that is calculated in the receiver side. The ALSP architecture that is proposed here uses both symmetric and asymmetric cryptography to provide all the aspect of network security such as Confidentiality, integrity, authentication, non-repudiation, availability and access control. The algorithm that is described above provides a good security under any environment and can be used as add-ins like IPsec.

V Simulation Results

Performance is the vital part of the TCP/IP Protocol suite. To demonstrate the performance for the proposed architecture, a series of simulation runs are performed on a variety of set of data. In our simulation, we use an Intel P-IV 1.60 GHz CPU, 512 Mb RAM in which performance result is collected Several performance metrics are used such as encryption time, Decryption time, CPU process time, CPU clock cycles and battery power. 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	*Data input size (Kb)*	*Original Architecture*	*ALSP Architecture*
1	25	25.40 ms	43.54 ms
2	60	42.25 ms	67.23 ms
3	100	61.43 ms	82.78 ms
4	250	74.04 ms	102.23 ms
5	1000	94.34 ms	125.32 ms
6	1250	156.24 ms	172.34 ms

From the analysis, it shows that the proposed architecture has slightly low 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.

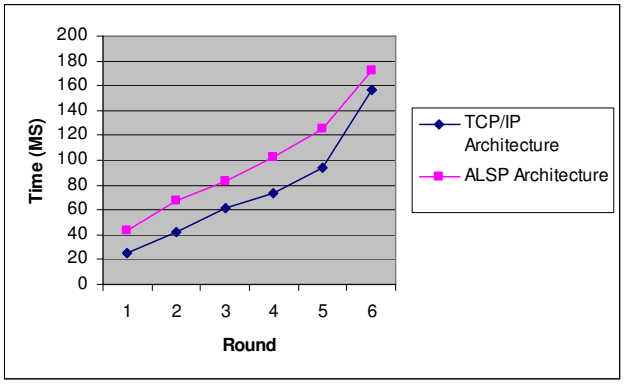

Figure 4. Performance Analysis

With the results from Figure 4, 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 IDEA and Elgamal were used. In this IDEA Encryption is taken for consideration. The IDEA algorithm is evaluated in such a way to reduce the execution time. In the near future we would modify the IDEA Encryption algorithm to reduce the execution time. But the security aspect of the proposed algorithm has improved a lot. Cryptanalysis is carried out in the encrypted file. It was found that the encrypted file with this algorithm is difficult to break.

VI Conclusion

This paper has outlined the need for security for the existing TCP/IP Model. It also provides 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.

VII REFERENCES

[1]. Behrouz A. Forouzan, TCP/IP Protocol Suite. New Delhi: Tata McGraw Hill Publication, 2003

[2]. Bradner, S., "The End-to-End Security," IEEE Security & Privacy, vol.2 no..4, pp, 76-79, 2006

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

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

[5]. Dorothy E. R. Denning, Cryptography and Data Security. Massachusetts: Addison-Wesley, 1982.

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

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

[8]. Hiromi, R.; Yoshifuji, H., "Problems on IPv4-IPv6 network transition," Proceedings of the internationalSymposium on Applications and the Internet Workshop, Saint 2005

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

[10]. 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

[11]. 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, 2004.

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

[13]. M.Mathis, "Reflections on the TCP Macroscopic Model", ComputerCommunication Review, volume 39, number 1, Jan 2009