ISSN 2250-3153

Next Generation of Internet Protocol for TCP/IP Protocol Suite

Miss. Soni Samprati

Department of Computer Science of Engineering
MIT Pune's, Maharashtra Academy of Engineering, Alandi(D).
Pune University, India
sonisamprati16@yahoo.com

Abstract- The Internet has instantly evolved into a vast global network in the growing techonology.TCP/IP protocol is the basic requirement for the recent time Internet .In TCP/IP proposed a security enhancement. This enhancement adds three modules. These are Security Policy, security control and data link layer. Security policy belongs to application layer, Security control is management located in the transport layer and Data security layer located between transport layer and IP layer. Security policy interacts with the system administrator for defining policies and roles of security to be applied in the data communications. Security control module provides the means to apply security policy module and established security channels. It usage four way handshaking and public key cryptography (PKC) to create virtual secure connection and secret key cryptography (SKC). Data security layer proposed Thin security over IP protocol. Thin security protocol encrypt and encapsulated the coming transport layer packet into TSP packets. 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 does not have any security provision in application layer and for security purpose there is a need for security mechanism. Here in TCP/IP architecture includes a layer called Security Layer, which guarantees security to provide Application layer using a protocol Application Layer Security Protocol.

Index Terms- Internet, TCP/IP, Security policy, Security control, Data Security Layer

I. INTRODUCTION

The emergence of IPv6 enables new generation of application and services. Security is traditionally connected to exigencies of defining sensitive data from illegal access. But in the moment network security is 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 corner stone for more and more network services. An increasing number of applications need multifaceted, consistent controls for guaranteeing Quality of service. Internet is based on TCP/IP protocol suite. IP was not planned with security in mind. TCP/IP suite is used for communication. It enabled million of computers to communicate globally.IPv6 is not designed to provide backward compatibility with IPv4, most IPv6 mission critical applications must be able to continuously interoperate with legacy IPv4 nodes. The most common transition mechanism now a days in Dual stack. A node with a dual stack allows co-existence and interoperability of IPv4 and IPv6 nodes using IPv4 and IPv6 packets. The gateway which is located at the boundary of IPv4 and IPv6 address real translates IPv4 header into IPv6 header or vice versa. To ensure end to end security between the end nodes, the deployment of IPSec since IPSec has been widely used in IP networks. AH header is inserted into the IP packet immediately after the outer IP header. Then, AH authentication the entire packet including the preceding IP header. The underlying of IPSec mechanism which preserve of translation gateway for most applications in the practices. When the translation gateway modifies the IP header from one address realm to another, IPSec evaluating this as violation of integrity and discards the packet. Therefore header from one address realm to another, IPSec evaluating this as violation of integrity and discard the packet. Here for TCP/IP suite security enhancement will be used. This enhancement adds three modules i.e. Security policy, security control and data security layer. The security policy belongs to application layer, and the security control and management located in the transport layer, the data security layer is located between the transport layer and IP layer. Security policy interacts with system administrator to define the policies and roles of security to be applied in data communication. Security control module provides the means to apply the security policy defined in security policy module and established a secure channel. It uses four way handshaking and public key cryptography (PKC) to create virtual secure connection and security entity (SE). SE holds the secret key cryptography (SKC) addresses of two host that share this SKC and other vital information necessary to carry out a secure data communication. For data security, proposed a thin security protocol (TSP) over IP protocol. TSP protocol encrypts and encapsulated the coming transport layer packet into TSP packets. The Tsp packet header consists only of two fields each of them is one byte. The first field identifies the TSP packets such as public key request, public key acknowledgement, secret key and secret key, and secret key acknowledgment. The second field carries information about the transport layer protocol.TSP designed and implementation, to concern minimize the overhead added to IP including traffic volume and transmission delay.

IPv6 is 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 to reach their correct destination. It holds great guarantee to become the backbone of the prospect of the internet and an important improvement over IPv4 in terms of scalability, security, mobility and convergence.

Existing or Related Work

The existing network layer protocol in the TCP/IP protocol suite is as present IPv4. IPv4/IPv6 translation gateway breaks IPSec. IPSec supports transport mode in providing end to end security between nodes. However, applying IPSec across translation gateway for this purpose violates TCP/UDP intrinsic functionalities. The co-existence of translation gateway and IPSec ESP is not feasible due to the IP header translation which cause the TCP/UDP checksum invalid.TCP/UDP checksum has a dependency on IP source and destination addresses through the inclusion of TCP/UDP pseudo-header in the calculation. Like normal Network Address Translation (NAT), while the translation gateway translates the IP address, it should also re-compute the checksum. Since IPSec ESP encrypt and authenticates ESP header and TCP/UDP header, any attempt to modify to checksum causes the integrity check to fail. Alternately, if translation gateway dose not update the checksum, TCP/UDP verification will fail. NAT-Traversal (NAT-T) is designed to solve the problems inherent in using IPSec and translation gateway. The following section extensively describes the operation of NAT. With NAT-T, the UDP-ESP encapsulation is deployed to support the IPSec packets from both end nodes to traverse the translation gateway and to avoid any problems with the IPSec aware gateway. Let's imagine multiple connections are mapped to one allocated address. Since IPSec ESP does not use port information, the translation gateway can only utilize the protocol field in IP header to distinguish the packets. When the first IPSec connection in the table so that all IPSec ESP packets will be routed to the first connection. However, when there is the new IPSec connection, the translation gateway replaces the entry in the table and thus breaking the first IPSec connection. UDP-ESP encapsulation gives the translation gateway an UDP header containing UDP port that can be used for multiplexing IPSec data streams.

Even though IPv4 is well designed, its security breaches make it inappropriate for the fast emerging Internet. To overcome these drawbacks, IPv6 also known as IPing was planned which became a standard in the recent past.

IPv6 Security Issues

From a security point of view, the new IPv6 protocol stack represents a considerable advance in reliable to the old IPv4 stack. However, despite its innumerable virtues, IPv6 still continues to be by far vulnerable. IPv6 where security continues to be an important issues:

- Dual stack related issues: Presently, the internet continues to be mostly IPv4 based. However, it is reasonable to expect that this scenario will change soon as more and more networks are migrated to be new protocol stack. Unfortunately, migrating millions of networks is going to take quite some time. In the mean time, some form of 6 to 4 dual-stack will supply the desired functionality without any doubt; IPv4-IPv6 dual stacks increase the potential for security vulnerabilities- as a consequence of having two infrastructures with specific security problems. However, most of the issues are not direct result of specific IPv6 design flaws but mostly a result of inappropriate configuration.
- Header manipulation issues: The use of extension and IPSec can deter some common sources of attack based on header manipulation. However the fact that EH must be proposed by all stacks can be source of trouble- a long chain of EH or some considerably large size could be used to overwhelm certain node an attack. Its uses source of security problems such as address spoofing- in this case if the spoofed address is used to masquerade an external packet as one that was originated from the inside network.
- Flooding issues: Scanning for valid host address and services is considerably more difficult in IPv6networks that it is in IPv4 networks. However, the larger addressing space does not mean that IPv6 is totally invulnerable to this type of attack. Nor the lack of broadcast address makes IPv6 more secure. New features such as multicast address continue to be source of problem.
- Mobility: Mobility is a totally new feature of IPv6 that was not available in this predecessor. Mobility is a very complex function that raises a considerable amount of concern when considering security. Mobility uses two types of addresses, the real address and the mobility address. The first is a typical IPv6 address contained in an extension header. The second is a temporary address contained in the IP header. Because of the characteristics of this networks, the temporary component of a mobile node address could be exposed to spoofing attacks on the home agent. Mobility requires special security measures and networks administrators must be fully aware.[1]

II. TCP/IP ARCHITECTURE

The TCP/IP protocol suite referred to as the Internet protocol suite, is the set of communication protocol that implements the protocol stack on which the internet and most commercial networks run. It is made up of two most important protocols in suite: the Transmission Control Protocol (TCP) and the Internet protocol (IP). Internet protocol is the foundation of the TCP/IP protocol suite, science it is the mechanism responsible for delivering datagram's. The TCP/IP protocol suite is like OSI Reference model which is defined as a set of layers. Upper layers are logically to the users and deal with more abstract data, relying on lower protocols to translate data into forms that are

transmitted physically over the network.TCP/IP suite which is the De facto standard for internet manages security with many other issues in the application layer making its a very thick one. Hence more, this means that the security problem needs to be solved by application developer whose consternation mainly on the main task of their application.

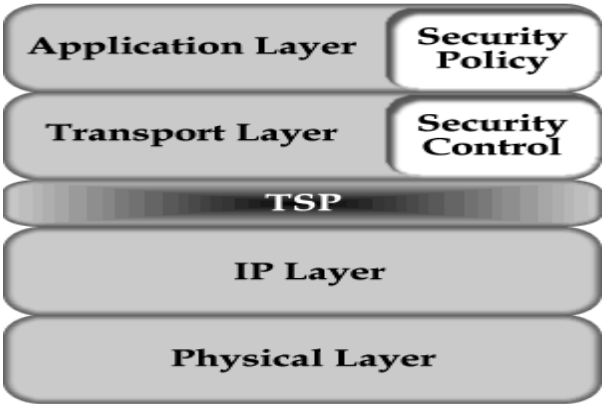

Figure 1: TCP/IP architecture

2.3.1. Security policy module:

Security policy module lies on the application layer with respect to TCP/IP protocol suite and interacts with user to define the proper security requirements. This security policy are stored and used by security control and management module to define the actions that should be accomplished for each communication session.

2.3.2. Security control and management module:

Security control and management module gets security requirements from its upper layer, which is security policy module. Based on the requirements, this module acts on each communication session .Security control and management module is responsible on providing the means required by data security layer. It creates a security entity(SE) for each communication session. SE contains an address of the sender, an address of the receiver, symmetric encrypt key, encryption algorithm, compressing algorithm, compressing enable and SE lifetime for which this SE will stay alive in security cache. Fig.2 [2] shows a four- way handshaking approach to establish a secure connection and exchange symmetric encryption keys between the sender and receiver.

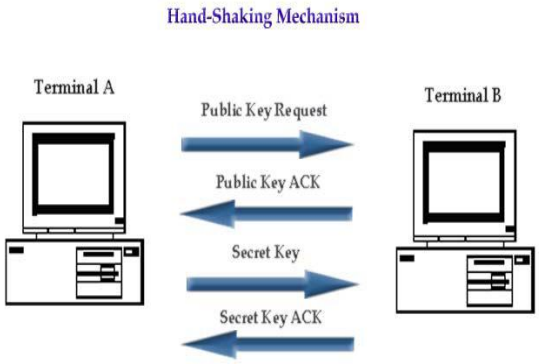

Figure 2: Exchanging symmetric encryption key using four-way handshaking

2.3.3. Data security layer:

Data security layer uses symmetric data encryption algorithm. The symmetric key used in this layer is provided by security control module. For each communication session there is security entity (SA). Hence more data security layer may uses data compressing algorithm to reduce the size of the encrypted data. We used data compressing because some encrypted algorithm output size is larger than input data the overhead added by compressing is accepted by security policy define by the system administrator. In fact the size is larger the input size in this case of the input size is small.

2.3.4. Thin security protocol:

Thin security protocols (TSP) intend to provide data security for all packets coming from transport layer. It encrypts transport layer packets using symmetric encrypt algorithm as shown in figure 1. The TSP header is only two bytes. The first one holds protocol vital information and the other preserve transport layer protocol type such as TCP or UDP.TSP two bytes header are specified in detail in figure 3.

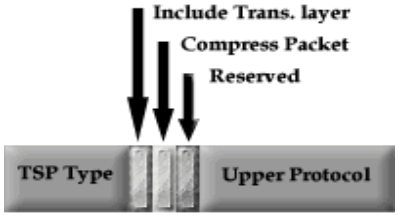

Figure 3: TSP Protocol Header

The first byte contain TSP type field, which is 5-bits long; it holds the type of TSP packet that is transmitted. TSP types are public key request, public key acknowledgment (ACK), secret key, secret key ACK, end connection, and end connection ACK packet. The rest of the first byte is used as indication flags, the first one which is denoted as “Include Trans. Layer” specifies wither this TSP packet has encrypted transport layer header or it is outside the encryption boundaries. The second bit denoted “Compress Packet” indicates if this packet is compressed. Compressing packet data is done after encrypting it. So it works as an indicator to allow the post-decryption handler to

decompress the received data. The last bit is reserved for future utilization. The second byte, which indicates the upper layer protocol, is an identical field to the one in the original IP header. The upper layer protocol field is filled with 255 to indicate that TSP protocol is used [3].

III. CRYPTOGRAPHIC ALGORITHM

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.

TABLE 1: Differentiate between these algorithms

Attributes	Blowfish	Elgamal	RC6	DES
Block size	64 bit	NA	NA	64 bit
Keys	Variable(32-448 bits)	One Secret key	Symmetric	Constant (56 bits)
Speed	Fast	Slower than Blow fish	Slower than Elgamal	Slower than Blow fish
Memory space	Large memory space	Comparatively less	Less	Less than Blow fish
Performance	Very Good	Good	Good	Good

A. Blowfish:

Blowfish 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.

Algorithm .1 (Encryption)

1. The input is a 64 bit data element, i.e. X.
2. Divide X into two 32 bit halves: XL,XR.
3. then 16 rounds Feistel network: for i=1 to 16:
4. XL=XL XOR Pi: for prevent the potential attack

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

5. XR=F(XL) XOR XR
6. After that swap XL and XR
7. swap XL and XR again to under the last swap
   After 1s6 round.
8. then XR=XR XOR P17 and XL=XL XOR P18
9. Recombine XL and XR to get cipher text.

TABLE 2: Dataset From Simulation

Decryption for Blowfish is relatively straightforward. Ironically, decryption works in the same algorithmic direction as encryption beginning with the cipher text as input. However as expected, the sub keys are used in reverse order[3].

IV. 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.

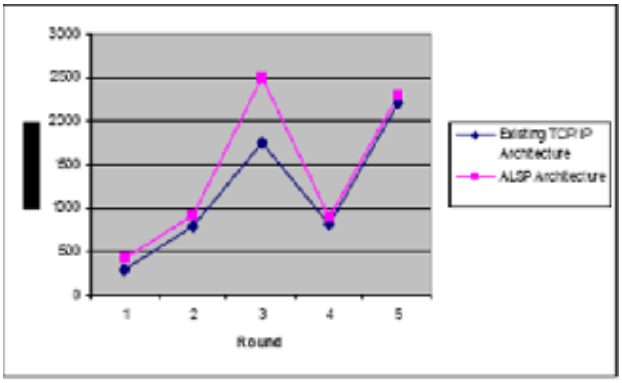

Fig 4: Performance Evaluation

From the previous one, 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[3].

Blow Fish Algorithm is fast, free alternative to existing encryption algorithm. It is slowly gaining acceptance as a strong encryption algorithm and also Unpatented, license free and available for all users. It uses sub keys that are a One-way hash function. In Blow fish, no linear structure therefore, it reduces the complexity of exhaustive search. And also it is easy to understand therefore here Blow fish algorithm would be used.

Here, We can modified to reduce the execution time Only that case performance of proposed system can be increased.

V. CONCLUSION

In this paper outlined several security problems of IPv6.It also outlined new ideas to design efficient security mechanism for the TCP/IP protocol suite. With some changes in the existing model, high level of security can be obtained. In this new structure of TCP/IP we added three modules. These modules are: Security policy, Security Control and Data security layer. It uses four way handshaking and Public key cryptography (PKC) to create virtual secure connection and security entity (SE). SE holds the secret key cryptography (SKC), and address of two hosts that share this SKC.TSP protocol minimizes the overhead added to IP including traffic volume and transmission delay. In term of data size, TSP adds only two bytes as TSP header. Hence more, TSP compress the encrypted data before sending it. It provides tight security with the minor overhead of the exiting model based on this Application Layer Security Protocol (ALSP) architecture.

ACKNOWLEDGMENT

My heartfelt thanks to my guide, Prof. R. M. Goudar, Asst Professor, College of Maharashtra Academy of Engineering, Pune, who offered her whole hearted guidance and invaluable suggestions throughout the preparation of 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] Samuel Sotillo, IPv6 Security Issues, East Carolina University.

[2] Mohammad Al-jarrah, Abdel-Karim R.Tamimi, Computer Engineering Department, Hijjah, Faculty for Eng. Techonology, Yarmouk University, Irbid 21163-Jordan.

[3] M.Anand Kumar, Security Model for TCP/IP Protocol Security, Karpagam University.

[4] Yongguang Zhang, A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks, Member, IEEE.

AUTHORS

Soni Samprati, M.E (1st year), Maharshtra Academy of Engineering, Pune
sonisamprati16@yahoo.com