International Research Journal of Management, IT & Social Sciences
Available online at https://sloap.org/journals/index.php/irjmis/
Vol. 3 No. 3, March 2016, pages: 53~64
ISSN: 2395-7492
https://sloap.org/journals/index.php/irjmis/article/view/354

IP Security

Saroj Singh [a]

Article history:

Received: 10 December 2015
Accepted: 30 January 2016
Published: 31 March 2016

Keywords:

Architecture;
Confidentiality;
Firewall;
Transport;
Tunnel modes;

Abstract

IP is stands for Internet Protocol. IP security is a set service which secures the documents by the unauthorized entity. IP Sec covers the three areas of functionality that is authentication, confidentiality, and key management. IP Sec encrypts and authenticates all the data traffic at the IP level security. The IP level security or firewall administrator, we got basically the same concerns (as plumber) the size of the pipe the contents of the pipe, making sure the correct traffic is in the correct pipes and keeping the pipes from splitting and leaking all over the places of course like plumbers. When the pipes do leak: we are the ones responsible for cleaning up the mess and we are the ones who come up smelling awful. Firewall is a device that is used to provide protection to a system from network based security threats. Firewall uses service, behavior, user and direction control techniques.

Author correspondence:
Saroj Singh,
Dept: Computer Science & Engineering Delhi Engineering College Ladiyapur, Faridabad, India,
Email address: sarojraj47@gmail.com , acme.singh10@gmail.com

1. Introduction

Definition: IP security is a set of services and not a protocol. IP Security, Bellovin, S. M. (1996, July), Endler, D., & Collier, M. (2006), covers three areas of functionality that that is authentication, confidentiality and key management. IP SEC encrypts and authenticates all the data traffic at the IP level.

a) Documents:
   The IP security covers many documents and was issued in November 2008. Some of the documents are listed below:
   1) REC 2401: It provides the overview of the security architecture.
   2) RFC 2402: It provides the description of the packets authentication that is the extension to IPv4 and IPv6.
   3) RFC 2406: It provides the description of the packet encryption that is the extension toIPv4 and IPv6.
   4) RFC 2408: It provides the specification of the key management.
b) IP security Architecture:
   1) Architecture: It covers the general concepts, security definitions, requirements and mechanism.
   2) ESP Protocol: ESP stands for Encapsulating security payload. It basically covers the packet format and issues related to the encryption and authentication process.

[a] Dept: Computer Science & Engineering Delhi Engineering College Ladiyapur, Faridabad, India

3) AH Protocol: AH stands for authentication header. It basically covers the packet format and issues related to the authentication process.

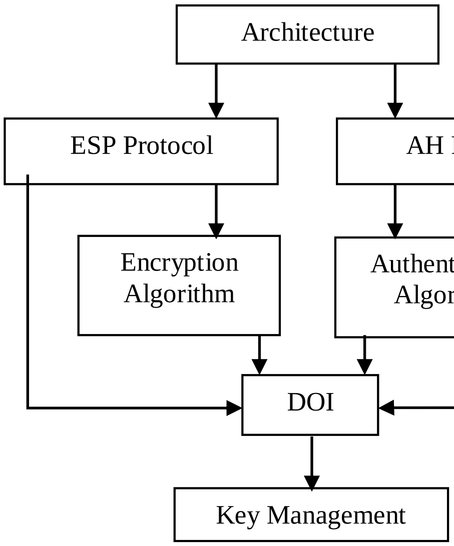

Figure 1. IP Security Architecture

1. Encryption Algorithm: It is a set of documents that describe how encryption algorithms are used for ESP.
2. Authentication Algorithm: It is set of documents that describe how authentication algorithms are used for AH. Hat are required for relating of documents.
3. Key management: It basically consists of documents that contain key management scheme.
4. DOI: DOI stands for domain of interpretation and contains values that are required for relating of documents.
5. Key Management: It basically consists of documents that contain key management schemes.

c) Applications:
1) Secure communication across LAN and internet.
2) Secure communication across public and private WAN and internet.
3) Secure branch office connectivity over the internet.
4) Secure remote access over the internet.
5) Secure Communication with organizations.

d) IP SEC Services:
1) Access control
2) Connectionless integrity
3) Authentication
4) Confidentiality
5) Limited traffic flow confidentiality

e) Transport and tunnel Model:
1) Transport and tunnel model are both supported by authentication header (AH) and encapsulating security payload (ESP) (Feit, 1998), Harris & Hunt, 1999).
2) Definition: transport mode provides protection to the upper layer protocols while tunnel mode provides protection to the inner IP packets.
3) Function of authentication header in transport mode: Authentication header authenticates IP payload and select portion of IPv4 and IPv6 header.
4) Function of authenticating security payload in transport mode: ESP encrypts IP payload and any IPv6 extension following the ESP header.
5) Function of authentication header in tunnel mode: Authentication header authenticates the entire inner IP packets and selected portion of outer IPV6 and IP header.

6) Function is encapsulating security payload in tunnel mode: ESP encrypts inner IP Packets.

f) Authentication Header:
Authentication header, Piper, D. (1998), Simpson, W. (1995), provides support for integrity and authentication of IP packets.

Next Header(8)	Payload Length(8)	Reserved(16)
Security Parameter Index(32)		
Sequence Number(32)		
Authentication Data		

Figure 2. Authentication Header

1) Next header: It identifies the type of header immediately following this header.
2) Payload lengths: the length of the authentication header 32 bit word minus 2.
3) Reserved: It is for the future use.
4) Security parameter index: this identifies the security associations.
5) Sequence Number: This is an increasing counter value.
6) Authentication data: this is a variable length field that contains integrity check value or message authentication code.

g) Encapsulating security payload:
Encapsulating security protocol provides confidentiality services.

Security Parameter Index(32)		
Sequence Number(32)		
Payload Data		
Padding(0-255)		
	Pad Length	Next Header
Authentication Data		

Figure 3. Encapsulating Security Payload

1) Security Parameter Index: It identifies security associations.
2) Sequence Number: this is an increasing counter value.
3) Payload Data: Here the transport and tunnel mode is protected by encryption.
4) Pad length: This indicates the number of pad bytes.
5) Next Header: this identifies the type of data in the payload data field.
6) Authentication data: This is of variable length containing integrity check value. The integrity check value is computed over authentication data field.

h) Key Management:
Definition: Key management is basically related to the identification and distribution of the secret keys. Authentication header and encapsulating security payload, Thayer, R., Doraswamy, N., & Glenn, R. (1998), consists of both transmission and receiving pairs.

Types of Key Management: These are two types:

1) Manual Key Management: Here the system configuration is manually performed by the administrator. The whole process is performed with its own keys and that of the communicating systems. This is basically meant for email systems and environments.
2) Automated key Management: Here the keys are created on demand and this is suitable for larger environments.
   (a) Oakley Key Determination Protocols: This is based upon the Diffie Hellmann and uses a mechanism called cookies. It the global specifies parameter of the Diffie Hellmann Key exchange and provides extra security.
   (b) Internet Security Association and Key Management Protocol (ISAKMP): It is basically consists of a set of message types and enable the use of variety of key exchange algorithm. It provides and formats to establish, negotiate, modify and delete security associations.

Benefits:

a) No training is required by the user on the security aspect.
b) It provides security for individual users if needed.
c) It provides greater security if implementation inside a firewall.

2. Research Methods

Firewall

Definition: Firewall is a device that is used to provide protection to a system or a set of system from network based security threats.

a) Characteristics of a Firewall
   1) Immune to operation
   2) Authorized traffic stated by the local security policy is allowed to pass through the firewall.
   3) Traffic flow both from inside to outside and outside to inside must pass though the firewall.

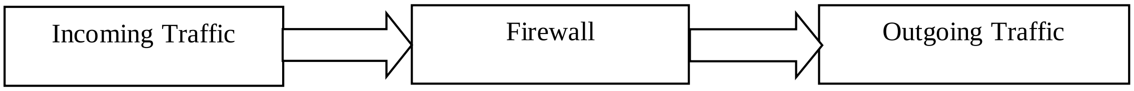

Figure 4: Traffic flow from Inside to Outside

Outgoing Traffic
Firewall
Incoming Traffic

Figure 5: Traffic flow from Outside to Inside

b) Technique used by Firewall

   There are four types of techniques used by the firewall.
   1) Service Control: These determine the types of services that can be accessed. The firewall filter traffic on the basis of internet protocol address and port number.
   2) Direction Control: It determines the direction in which a particular service request provided by the service control can be initiated and allowed to pass through the firewall.
   3) User Control: This is applied to the users inside the firewall and is applied to the incoming traffic from external users.
   4) Behavior Control: It controls how particular services can be used.

c) Architecture of Firewall:
The characteristics of firewall can be classified as:

1) Single Layer Architecture:
In single Layer architecture, a single host is allots all firewall functions. This architecture is only used when cost is a factor or two networks are to be connected. It provides a single entry point.
Advantage: any charge to the firewall needs to be done only at the single host.
Disadvantage: If the single entry point is reached then the entire networks becomes susceptible to the attack.
2) Multiple Layer Architecture: In multiple layer architecture, the firewall functions are distributed among hosts that are connected in series.
Advantages: Multiple architecture provides greater security.
Disadvantaged:
(a) These are difficult to design and manage.
(b) These are more costly.

Design approach of firewall: for multiple layer architecture Demilitarized network (DMZ) is used. The demilitarized network separates the internet and internal network. The traffic should pass through two firewalls and DMZ is multiple layer architecture.

d) Capabilities of firewall

1) Firewall provides location for monitoring security related events.
2) Alarms can be implemented on the firewall system.
3) Firewalls are a platform for IP Sec.
4) Firewall keeps unauthorized users out of the protected network.

e) Limitations of Firewall

1) It provides location no protection against virus infected files.
2) It provides no protection against internal threats.

f) Operation of Firewall

Firewall operates at the third layer in the OSI model. This layer is known as the network layer. Firewall operated at the internet protocol for TCP/IP.

Firewall operating at the highest layer called application layer knows about a large amount of information.

1) Secure content
2) Packet content

Bastion Host:

It is a system identified by the firewall administrator and is a crucial aspect in the network security systems. It executes a secure version of the operating system and requires additional authentication before the user can access the services. For example: Telnet, FTP, and SMTP.

g) Configuration of Firewall
The configuration of firewall can be elaborated in three parts:

1) Screened HOST Firewall Single Homed System: This consists of two system packets filtering router and bastion host. Here traffic flows in two ways:
(a) Traffic from the internet: IP Packets destined for the bastion host are allowed in.
(b) Traffic from the internal network: IP packets from the bastion house are allowed out.
2) Advantages:
(a) Two level of security.
(b) It provides flexibility.
3) Screened host Firewall Dual Homed Bastion System: The host can directly communicate with the router.
4) Screened subnet firewall System: Two packets filtering routers are used. First is between the bastion host and the internet and second is between the host and the internal network.
Advantages:
(a) Provide three level of security.
(b) Internal network is invisible to the internet.
(c) Internet is invisible to the internal network.

h) Types of firewall

There are three types of firewall.

1. Packet Filtering Router: In this type of firewall a set of rules are applied to reach incoming IP Packet and then it is decided to either forward the packet or discard the packet. The router is basically configured to filter both the incoming and outgoing packets. Packet filtering router consists of:
2.

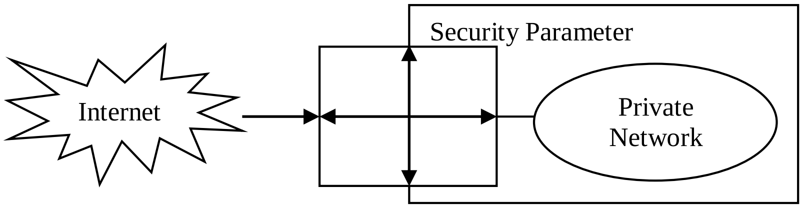

Figure 6: Packet Filtering Router

a) Source IP address: This is the IP address of the system that originated the IP packet.
b) Destination IP Address: This is the IP address of the system that the IP packet is trying to reach.
c) Source and destination transport level address: This is the port number that defines applications such as SNMP or Telnet.
d) IP Protocol Field: This defines the transport protocol.
e) Interface: This is the interface through which the packet came or the packet is destined distinct to.

Advantages:

a) Simplicity
b) Low Cost
c) Client computers can be used directly. There is no need for special configuration.

Disadvantages:

a) No support of advanced user authentication schemes.
b) Prone to attacks.
c) Improper configuration may lead to security problems.
d) No protection against application based attacks.
e) Packet filtering routers cannot perform content based decisions.
f) These are hard to direct if the network is susceptible to attacks.
g) They do not store the state of the connection. Thus these are stateless.
h) Testing of grant and deny rules is difficult making the network incorrectly configured.

3. Application Level Gateway: This firewall acts as the relay of application level traffic and is also called Proxy Server. The user contacts the application level gateway using a TCP/IP [5] application such as telnet or FTP. These are the third generation of firewall architecture. It was created by Gene Spafford of Puredue University, Marcus Ranum and Bill Cheswick of AT&T Bell Laboratory.

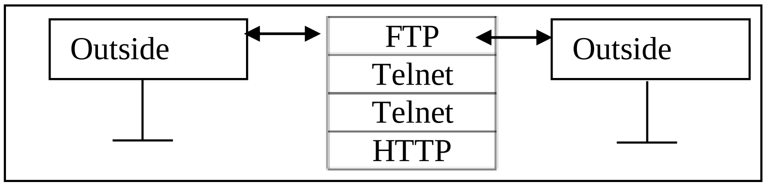

Figure 7: Application Level Gateway

Application Level Gateway contains two primary modes. These are

1. Proxy Server
2. Proxy Client

Gateway asks the user to provide the information regarding the name of the remote host to be accessed. If the user provides with a valid ID and authentication information the gateway contacts the application on the remote host and relays TCP segments containing the application data to the user.

Advantage:

a) It is secured than packet filtering router.
b) These store the information about the data which passes through the firewall server.

Disadvantages:

a) Requires additional processing overhead of each connection.
b) Complex filtering
c) Performance delay occurs.
d) These are prone to operating and application bugs.
e)

4. Circuit Level Gateway: The circuit level gateway sets up two connections. First is between the circuit level gateway and the TCP user on the inner host and second is between the circuit level gateway and the TCP user on the outer host. The gateway relays TCP segments from one connection to another without examining the contents. This type of firewall is used in a situation in which the system administrator trusts the internal users. Example: SOCKS package consisting of the socks and socks client library.

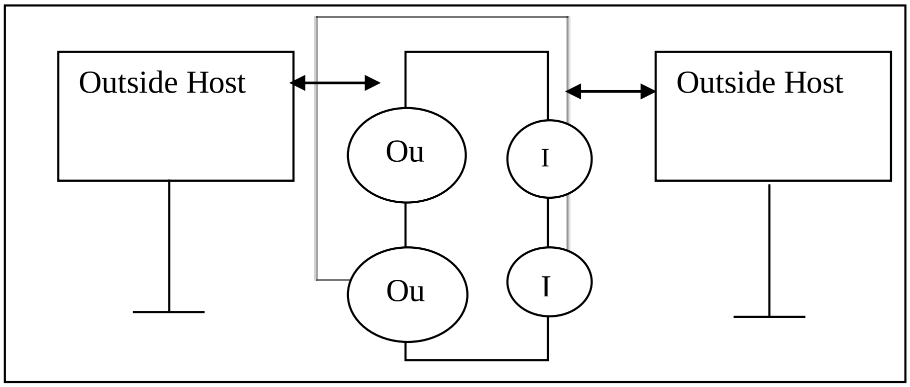

Figure 8: Circuit Level Gateway

Uses:

a) These are used to store unique session identifier.
b) These store the state of the connection.
c) These also store the source and destination IP address.
d) These also store the information that is sequenced.

Advantages:

a) These are faster than the application level firewalls
b) Less evaluation is required.
c) These protect the network by blocking the connections between the internet sources and internal hosts.

Disadvantages:

a) Circuit level gateways cannot restrict the access to the protocol subsets.

3. Results and Analysis

3.1 Secure socket layer and transport layer security

Definition: secure socket layer was develop by Netscape and is a protocol that is used for managing secure message transmission over the internet. The version 3 of the protocol was designed on the basis of the input from the industry and users. It was published as an internet draft document.

Transport layer security is an extension of the secure socket layer.

a) *Architecture*

This layer consists of two protocols and uses transmission control protocol to provide reliable and secure services.

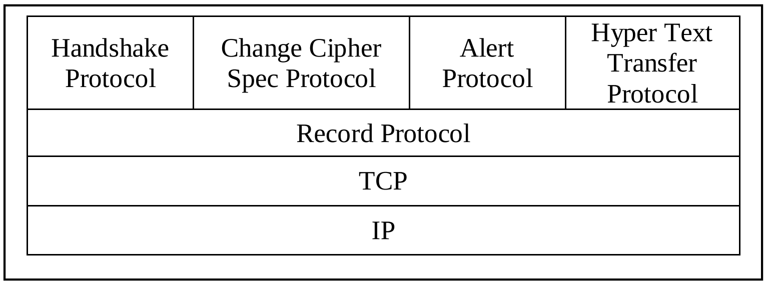

Figure 9. Architecture of SSL

Handshake Protocol: this is used before any data or application can be transmitted and allows server and client to authenticate each other. The message has three protocols:

1) Type: Type indicates one of ten handshake protocol message types.
2) Length: this is indicated in bytes.
3) Content: This is the parameter which is associated with each message.

Action: The action of the handshake protocol is divided into four phases:

1) Phase 1: Establish security capabilities, including protocol version, session ID, cipher suite, compression method and initial random numbers. Establish hello message phase.
2) Phase 2: server may sends certificate, key exchange and request certificate. Server signals end of hello message phase.
3) Phase 3: client sends certificate if requested. Client sends key exchange. Client may also send certificate verification.
4) Phase 4: Change cipher suite sand finish handshake protocol.

Change Cipher Spec Protocol: Spec stands for specific and thus it is a secure socket layer specific protocol. This consists of a single message containing only a single byte. Its role is to copy the pending state into current state.

Alert Protocol: it is used to stands alerts to the entity. The alert can be of the following types.

1) Unexpected message
2) Handshake Failure
3) Decompression failure
4) Expired certificate
5) No certificate available
6) Corrupt certificate

The alert is of two bytes. The first byte symbolizes warning while the second byte denotes failure that the connection is terminated.

Hyper Text Transfer Protocol: This is topmost layer of SSL and is a transfer service for the web client and server.

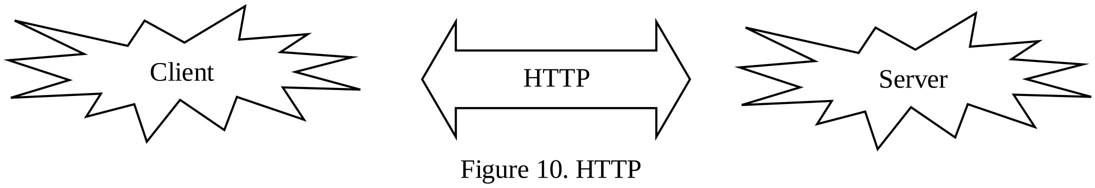

Figure 10. HTTP

Record protocol: It is used to provide confidentiality and integrity of the message to the connection.

b) *Operations*

1) Fragment the application data
2) Compress the fragment data
3) Add the message authentication code to the compressed and fragmented data
4) Encrypt the data

5) Appended the record header to the message to be transmitted.

c) Format

Content Type (8)	Major Version (8)	Minor Version (8)	Compressed Length (16)
Plaintext			
Message Authentication Code			

Figure 11. Format of SSL

d) Concepts in SSL

SSL uses two concepts that is connection and session. Connection: it is a peer to peer service in SSL and each connection is associated with only one session. The parameters used are:

1) Random Server: The byte sequences are selected by the server for connection.
2) Random client: The byte sequence is selected by the client for connection.
3) MAC secret by server and client: The secret key used in message authentication code (MAC)is written by client and server respectively
4) Encryption key by client: The encryption key used to encrypt the data is written by the client and decrypted by server.
5) Encryption key by the server: the encryption key used to encrypt the data is written by the server and decrypted by client.

Session: It is an association between the client and server and is created by handshake protocol. Each session can be associated with more than one connection. The two states associated with session concept are read and write. The parameters used are:

1) Session Identifier: It is an arbitrary sequence chosen by the server to identify states. The states can either be worked or on resume.
2) Certificate: This is X 509.v3
3) Compression Method: The method is used to compress data before encryption.
4) Is-Resumable: Temporary variable is used to indicate whether the session can be used ro initiate new connection.
5) Master secret: It is shared between the client and server and is of 48 byte.

3.2 Secure Electronic Transaction (SET)

Definition: SET is an open encryption and security specification [7] designed to protect credit card transaction on the internet in a secure and efficient manner the initial specification of SET was developed with the help of many companies like IBM, Microsoft, etc.

a) Participants in SET

The following are the participants:

1) Consumer: Consumer is authorized holder of the payment card that issued by the issuer and interacts with the merchant over the internet.
2) Merchant: Can be a person or a complete organization that provides goods and services to the consumer via email or website.
3) Issuer: Financial institution such as bank that provides credit card to the consumer and is responsible for the payment of the debt of the consumer.
4) Acquirer: Financial institution that provides an account to the merchant and enables electronic transfer of payment to the merchant account.
5) Payment Gateway: It is an interface between the SET and payment network. This is operated by the acquirer or any other third party and processes merchant payment messages.

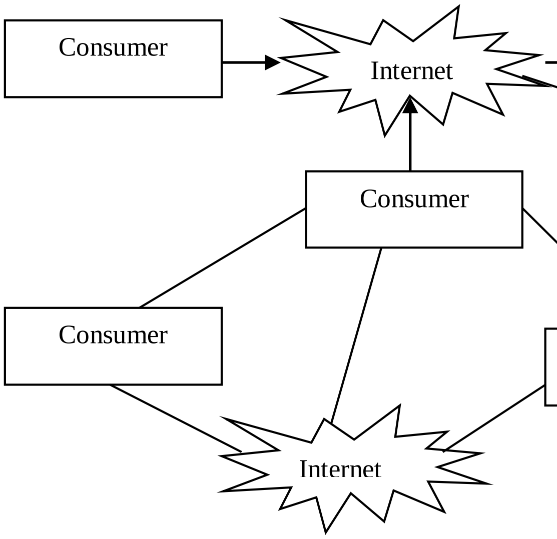

Figure 12. SET

b) Features
1) Confidentiality: It is done though DBS and prevents s the merchant from learning the cardholder’s credit numbers.
2) Integrity: It is done through RSA [8] digital signature scheme and assures that the personal information of the consumer will not be altered.
3) Authentication: The authentication [9] is done on both the consumer and merchant part. X.509v3. Authentication is done to verify that both consumer and merchant are legal. There are some steps followed by consumer and merchant both. Some steps are:
(a) Consumers open an account and receive a certificate.
(b) Merchant have their own certificates and verification is performed.
(c) Customer paces an order and payment is sent.
(d) Merchant confirms order and requests payment authorization.
(e) Merchant provides services and obtain payments.

c) Transaction types
1) Consumer registration: Consumer has to register with the certificate authority before they can send electronic transfer –Y message to merchant.
2) Merchant Registration: Merchant must register with the certificate authority before they can send goods to consumer.
3) Purchase request: It is the message from the consumer to the merchant containing order information for the merchant and purchase information from the bank.
4) Payment authorization: Authorization of the amount of purchase on the given credit card amount.
5) Payment capture: Allows merchants to capture their payments from the payment gateways.
6) Credit: Allows a merchant to issue credit to cardholder’s account when damaged are inappropriate goods are returned.

4. Conclusion

IP is stands for Internet Protocol. IP security is a set service which secures the documents by the unauthorized entity. IP Sec covers the three areas of functionality that is authentication, confidentiality, and key management. IP Sec encrypts and authenticates all the data traffic at the IP level security. The IP level security or firewall administrator, we got basically the same concerns (as plumber) the size of the pipe the contents of the pipe, making sure the correct traffic is in the correct pipes and keeping the pipes from splitting and leaking all over the places of course like plumbers.

Conflict of interest statement and funding sources

The author(s) declared that (s)he/they have no competing interest. The study was financed by personal funding.

Statement of authorship

The author(s) have a responsibility for the conception and design of the study. The author(s) have approved the final article.

Acknowledgments

Nobody can do anything without the grace of God. I first thank to “Lord Krishna” and “OMKAR” who blessed me to achieve my ambition by writing this research paper named “IP Security”. I am thankful to almighty God for blessing me with the strength to face any situation with courage and patience. I extended my thanks to my dear husband who encourage me finish the task successfully on time. I also thanks to my parents for their inspiration and blessings.

a) I also thank to my children and my in-laws who supported me for accomplishing my goal.
b) I would also like to thank my friends and my colleague who supported me in each step. I would like to thank my publishers who gave me the golden opportunity to write this research paper.

References

Bellovin, S. M. (1996, July). Problem Areas for the IP Security Protocols. In *USENIX Security Symposium*.

Endler, D., & Collier, M. (2006). *Hacking exposed VoIP: voice over IP security secrets & solutions*. McGraw-Hill, Inc..

Feit, S. (1998). *TCP/IP: Architcture, Protocols, and Implementation with IPv6 and IP Security*. Computing McGraw-Hill.

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer communications*, *22*(10), 885-897.

Piper, D. (1998). *The internet IP security domain of interpretation for ISAKMP* (No. RFC 2407).

Simpson, W. (1995). IP in IP tunneling.

Thayer, R., Doraswamy, N., & Glenn, R. (1998). *IP security document roadmap* (No. RFC 2411).