IPv6 Security Considerations

Mohammad Heidari
Babisandz@yahoo.com

ABSTRACT

IP version 4 has played a main role in the interworking environments for many years, it has proved flexible enough to work on many different networking technologies and however it has become a victim of its own success – explosive growth! - In the 1990s the "World Wide Web "and personal computers shifted the user of the Internet to the general public. This change has created heavy demands for new IP addresses; the lake of IPv4 addressing space was the basic problem. In the early 1990s IETF began to work on the IPv4 for solving the address exhaustion and other scalability problem .After several proposals were investigated a new IP version was recommended in late 1994 , the new version is called IPv6 (also called IPng: IP next generation). IPv6 uses a 128 bit IP address made up at eight 16 bit integers separated by colons; IPv6 contains many new features including native security. In this article I try to explain IPv6 security concepts.

September 2, 2004

Introduction to IP next generation

IPv6 retains many of the design features that have made IPv4 so successful. Some of the changes from IPv4 to IPv6 include:

1- Address size: The length of address field is extended from 32 bits to 128 bits; the address structure also provides more level of hierarchy. With the increased IP address size, the address space can support to 3.4 * 10^38 hosts.

2- Simplified header format: the IPv6 datagram header is completely different than the IPv4 header, some of the header fields in IPv4 such as check sum, IHL, identification flag and fragment offset do not appear in the IPv6 header.

3- Extension header: IPv6 encodes information into separate headers, this features is called flexible support for option.

4- Flow label capability: IPv6 adds a “flow label “to identify a certain packet flow That requires a certain quality of service.

5- Fragmentation at source only: Routers do not perform packet fragmentation if a packet needs to be fragmented, the source should check the minimum MTU along the path and perform the necessary fragmentation.

6- Support for audio and video: IPv6 includes a mechanism that allows a sender and receiver to establish a high quality path through the underlying network and to associate Datagrams with the path. Although the mechanism is intended for use with audio and video applications that require high performance guarantees, the mechanism can also be used to associate Datagrams with low-cost paths.

7- No checksum field: the checksum field has been removed to reduce the packet processing time in a router, Packets carried by the physical network are typically already checked, furthermore, high-layer protocol such as TCP and UDP also perform their own verification, thus the removal of the checksum field is unlikely to introduce a serious problem in most situations.

8- Large packets: IPv6 supports payloads that are longer than 64 Kbytes.

9- Extensible protocol: Unlike IPv4, IPv6 does not specify all possible protocol features, instead the designers have provided a scheme that allows a sender to add additional information to a datagram .the extension scheme make IPv6 more flexible than IPv4 , and means that new features can be added to the design as needed.

10- Security: IPv6 supports built-in authentication and confidentiality.

IP Security

IP security provides security mechanism to (IPv4 or IPv6). It includes a set of facilities that support security services such as authentication, integrity, confidentiality and access control at the IP layer. We can use IP Security in two ways:

1- Transport mode: implemented directly between remote systems but remote systems must support IP Security

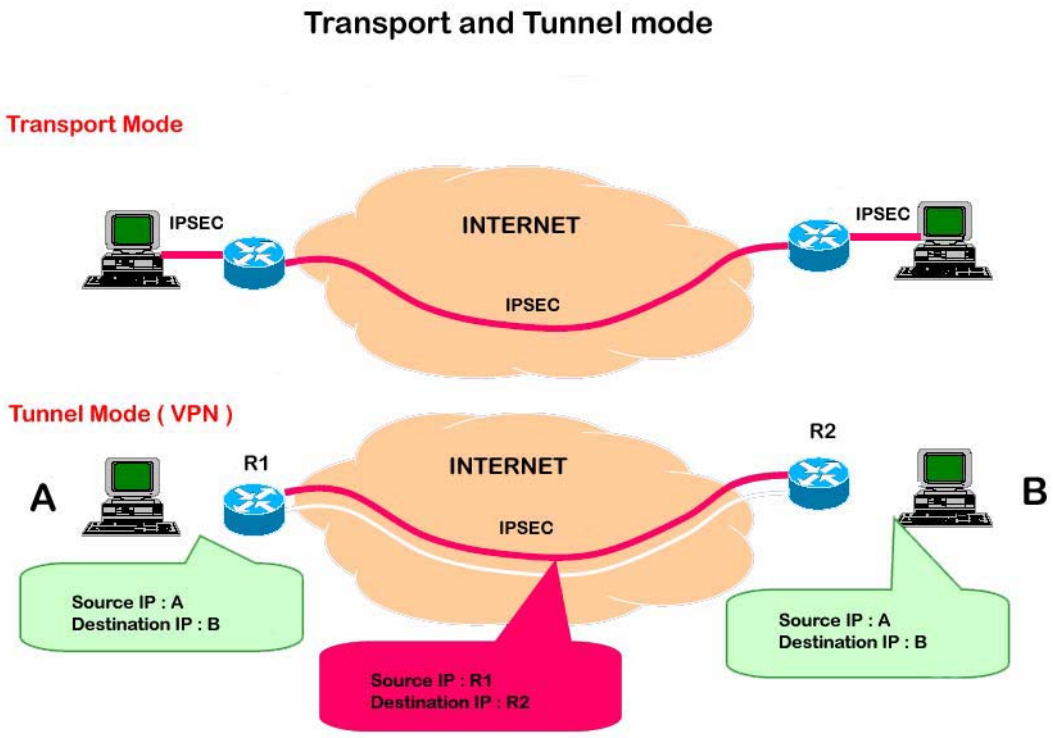
2- Tunnel mode: implemented between intermediate systems that is used for encapsulating insecure IP datagrams.

Transport mode and Tunnel mode by figures:

IP datagram

IP Security Datagram (Transport Mode)

IP Security datagram (Tunnel Mode)



How is IP Security transmitted?

IP Security adds a new header in the IP datagram between the original header and the payload .In ESP, data are encrypted and a new datagram trailer is added.

IP Datagram

IP Security Datagram

IP security has four main functionalities:

1- Security Associations (SA)
2- Authentication only (Authentication Header or AH)
3- Encryption and authentication known as Encapsulating Security Payload (ESP)
4- Key management

1- Security Association (SA)

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the SA. An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relation is needed for two way secure exchange, then two security associations are required .Security services are afforded to an SA for the use of AH or ESP, but not both. A security association is uniquely identified by three parameters:

1- Security Parameter Index (SPI): Bit string assigned to the SA with local meaning, it is Transmitted in the AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

2- IP Destination Address: it supports only Unicast (The address corresponds to a single computer) addresses

3- Security Protocol Identifier: This indicates whether the association is an AH or ESP security association

Hence, in any IP packet (IPv4 datagram or an IPv6 packet) the security association is uniquely identified by the destination address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP). A Security Association is normally defined by the following Parameters:

1- Sequence Number Counter: A 32-bit value used to generate the sequence number field in AH or ESP headers

2- Sequence Counter Overflow: A flag indicating whether of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA

3- Anti Reply Window: Used to determine whether an inbound AH/ESP packet is a reply

4- AH Information: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.

5- ESP Information: Encryption and Authentication Algorithm, keys, initialization values key lifetimes, and related parameters being used with ESP
6- Lifetime of this security association: A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur

7- IP Security Protocol mode: Tunnel, Transport (required for all implementations)

8- Path MTU: Any observed path maximum transmission unit

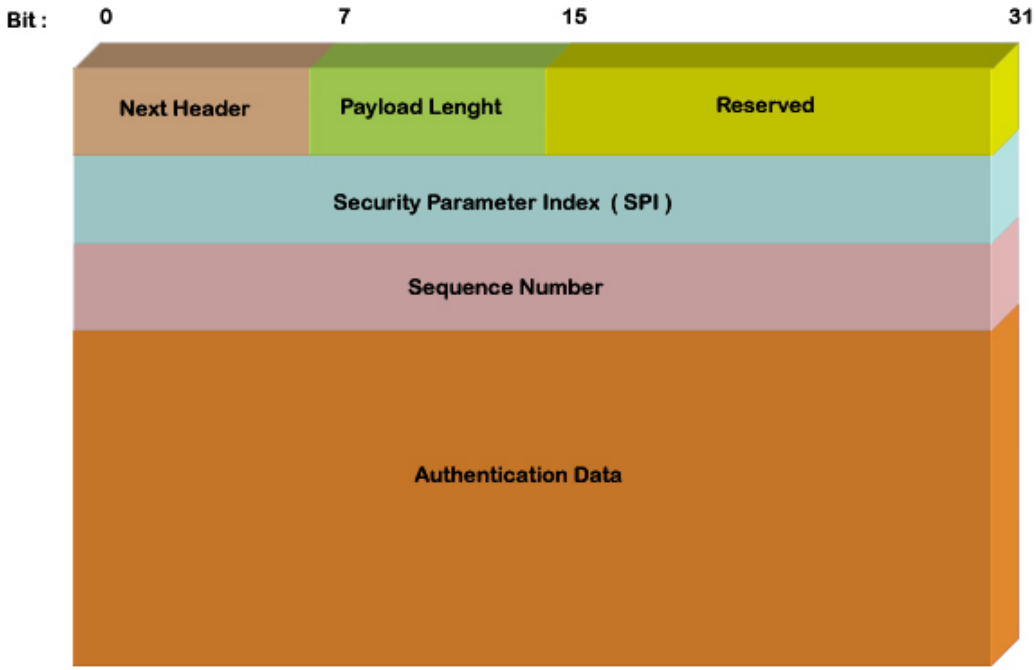
As mentioned earlier Both Authentication Header and Encapsulating Security Payload support the Transport and Tunnel modes (IP Security supports two modes) this table summarizes transport and tunnel mode functionality:

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extensions header	Authenticates entire inner IP packets and selected portions of outer IP header and outer IPv6 extensions header
ESP	Encrypts IP payload and any IPv6 extensions headers following the ESP header	Encrypts inner IP packets
ESP with Authentication	Encrypts IP payload and any IPv6 extensions headers following the ESP header, Authenticates IP payload but not IP header	

2- Authentication Header (AH)

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP Datagrams and to provide protection against replay attack. AH is based on the use of the integrity check value with an algorithm specified in the SA. It avoids IP-Spoofing attack.

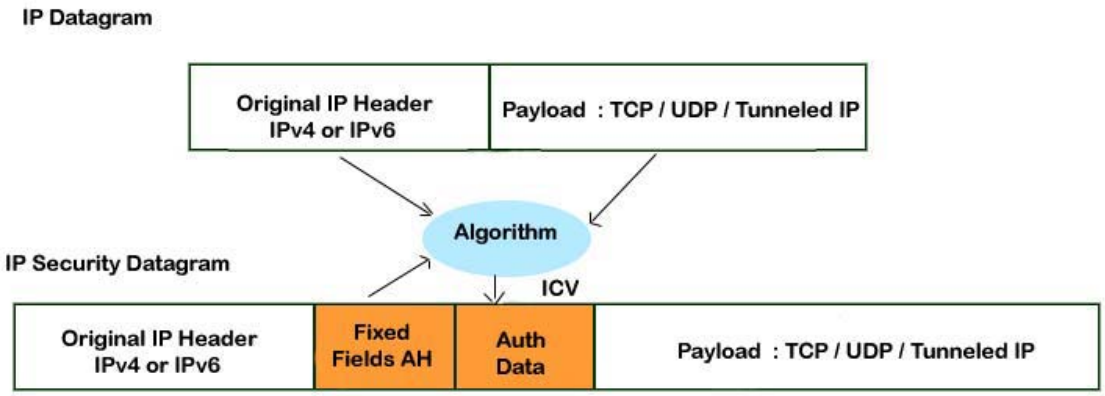
IP Security Authentication Header



Authentication Header consists of the following fields:

1- Next Header: Data protocol transmitted inside IP (e.g. TCP, UDP, etc.)
2- Payload length : Length of Authentication Header
3- Security Parameter Index (SPI) : Identification of the SA of this datagram
4- Sequence Number : Counter monotonically incremented with each packet
5- Authentication Data : it contains the Integrity Check Value (ICV)
6- Reserved: (16 bits) for future use

But what is "Authentication Data "?

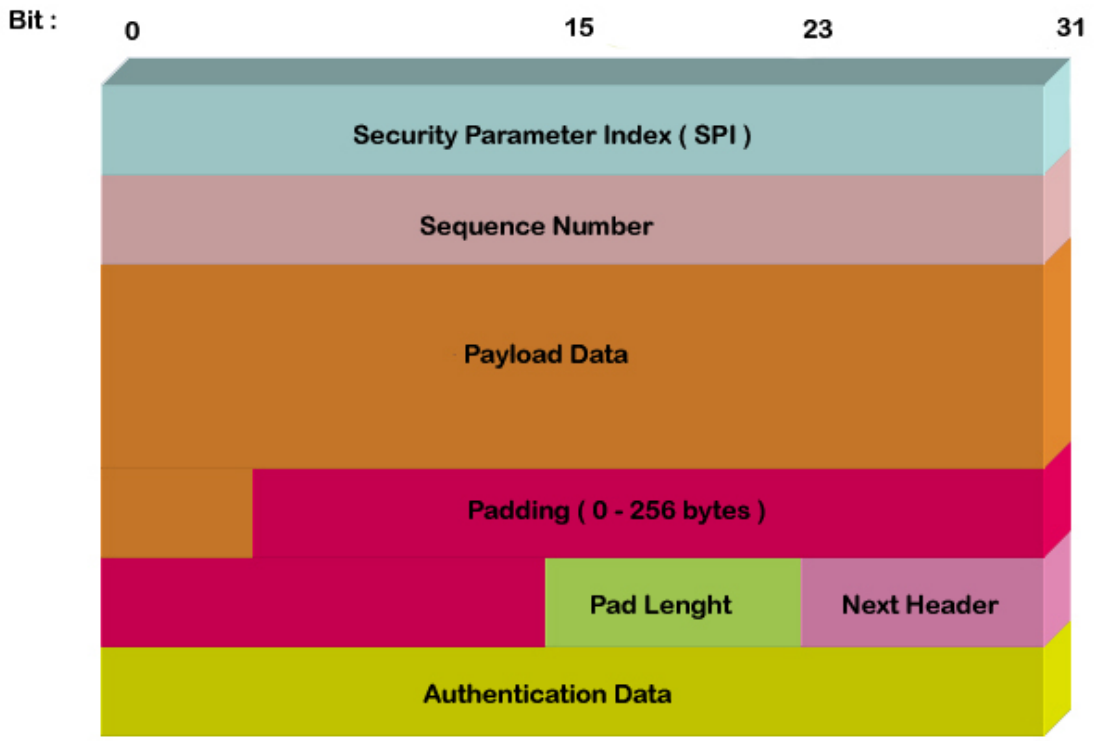


What is Reply Attack and How does AH prevent it?

A reply attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, Authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The sequence number field is designed to thwart such attacks .When a new SA is established, the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the sequence number field. Thus, the first value to be used is 1.If anti-reply is the enabled sender must not allow the sequence number to cycle past 2^32 – 1 back to zero. Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 2^32 – 1 is reached, the sender should terminate this SA and negotiate a new SA with a new key. Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IP security authentication document dictates that the receiver should implement a window of size W, with a default of W=64.The right edge of the window represents the highest sequence number in the range from N-W+1 to N that has been correctly received .

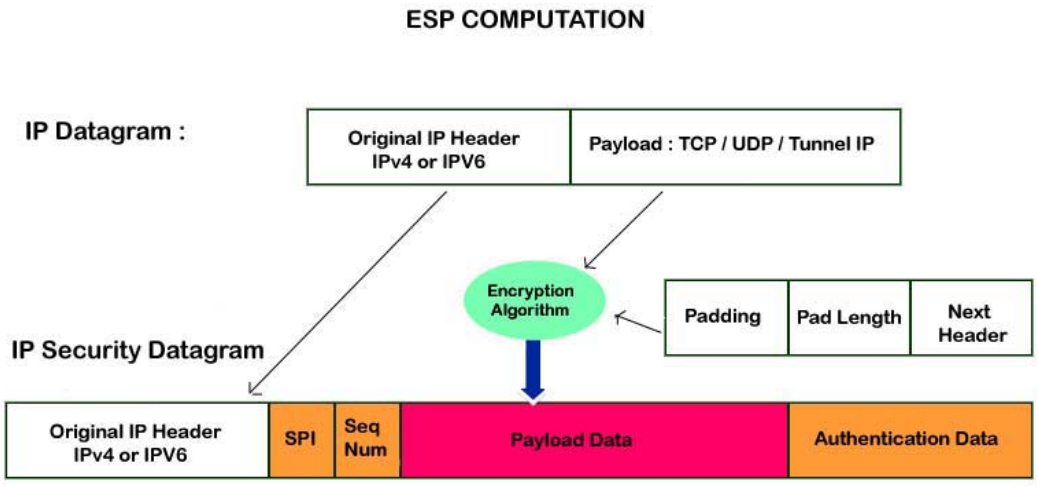
3- Encapsulating Security Payload (ESP)

The Encapsulating Security Payload provides confidentiality, authentication, and data integrity. An ESP can be applied alone or in combination with an AH.



Encapsulating Security Payload includes:

1- Security Parameter Index (SPI): Identification of the SA of this datagram
2- Sequence Number : Counter which is incremented with each packet
3- Payload Data : Encrypted Data of the IP protocol
4- Padding : Extra bytes needed if the encryption algorithm needs complete text blocks
5- Pad Length : Number of padding bytes
6- Next Header : Data protocol in the payload data
7- Authentication Data : ICV computed over all the datagram (Except Authentication Data Field)



Limitations:

The AH and ESP do not provide security against traffic analysis, It is not economical to provide protection against traffic analysis at the IP layer. One approach in the protection against the traffic analysis is the use of bulk link encryption, another technique is sending false traffic in order to increase the noise in the data listened by the traffic analyst .AH or ESP do not provide non-repudiation when used with the default algorithms . Use of certain algorithm for example RSA with appropriate transformation provides non-Repudiation. Non-Repudiation should be concerned with the application layer security.

4- Key management

The key management portion of IP Security involves the determination and distribution of secret keys. The IP Security architecture document mandates support for two types of key management:

1- **Manual:** A system administrator manually configures each system with its own keys and the rest of system's keys; this is practical for small and static environments.

2- **Automated:** An automated system enables the on-demand creation of keys for Security Associations and facilities, the use of keys in a large distributed system with an evolving configuration.

The default automated key management protocol for IPSEC is referred to as ISAKMP/Oakley and consists of the following elements:

1- Oakley Key Determination: Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.

2- Internet Security Association and Key Management Protocol (ISAKMP): ISAKMP provides a framework for Internet Key management and provides the specific protocol support, including formats, for negotiation of security attributes.

1- Oakley Key Determination Protocol

Oakley is a refinement of the Diffie-Hellman key exchange algorithm. Diffie-Hellman involves the following interaction between users A and B:

- **q** is a large primus number
- **α** is a primitive root of **q**
- **A** selects a random integer **X(A)** (Secret Key) and transmits to **B** : **Y(A)= α.X(A)**
- **B** selects a random integer **X(B)** (Secret Key) and transmits to **A : Y(B)= α.X(B)**
- each side can now compute the secret session key :

K=Y(B)^X(A) mod q= Y(A)^X(B) mod q

The Diffie-Hellman algorithm has two attraction features:

1- Secret keys are created only when needed, there is no need to store secret key for a long period of time, exposing them to increased vulnerability

2- The exchange requires no preexisting infrastructure other than an agreement on the global parameters.

However there are a number of weaknesses to Diffie-Hellman as painted out in [HUTT98]:

1- It does not provide any information about the identities of the parties

2- It is computationally intensive. As a result, it is vulnerable to a clogging attack in which an opponent requests a high number of keys. The victims spends considerable computing resources doing useless modular exponentiation rather than real work

3- It is subject to man-in-the-middle attack , in which a third party C impersonates B while communicating with A and impersonates A while communicating with B. Both A and B end up negotiating a key with C, which can then listen to and pass on traffic

Oakley is designed to retain the advantages of Diffie-Hellman while countering its weaknesses .The Oakley algorithm is characterized by five important features:

1- It employs a mechanism known as cookies to thwart clogging attacks.
2- It enables the two parties to negotiate a group.
3- It uses nonces to ensure against reply attacks.
4- It enables the exchange of Diffie-Hellman public key values
5- It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks

2- ISAKMP

ISAKMP defines procedures and packet formats to establish, negotiate, modify, and delete security association as part of SA establishment, ISAKMP defines payloads for exchanging key generation and authentication data. These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism. An ISAKMP message consists of an ISAKMP header followed by one or more payloads. The header format of ISAKMP message consists of Initiator Cookie (64 bits), Responder Cookie (64 bits), Next Payload (8 bits) , Major Version (4 bits), Minor Version (4 bits)Exchange Type (8 bits), Message ID (32 bits), Length (32 bits)

ISAKMP Exchange

ISAKMP provides a framework for message exchange, with the payload types serving as the building blocks. The specification identifies five default exchange types that should be supported.

1- **Base Exchange** Allows key exchange and authentication material to be transmitted together.

2- **Identity Protection Exchange** expands the Base Exchange to protect the user's identities. (First key exchange then Authentication)

3- **Authentication Only Exchange** is used to perform mutual authentication, without a key exchange

4- **Aggressive Exchange** minimizes the number of exchanges at the expense of not providing identity protection

5- **Informational Exchange** is use for one-way transmittal of information for SA management

CONCLUSION

This paper explains the main aspects of IP security in IPv6. SA, AH, ESP, and key management are discussed in this article. IP Security may solve many issues on the Internet such as : FTP , Telnet , DNS , and SNMP but other security issues exist : IP security tunnels break through firewall or NAT or tunneled IP security traffic may contain malicious data . QOS does not work in IP security, Dynamic IP addresses cause IP security to fail.

AKNOWLEDEGMENT

I am grateful to Zahra Heidari for her efforts in editing this paper, and special thanks to my brother “Vahid” for his technical support

References

[1] **R. Atkinson.** Security Architecture for the Internet Protocol, RFC2401
[2] **R. Atkinson.** IP Authentication Header (AH), RFC2402
[3] **R. Atkinson.** IP Encapsulating Security Payload (ESP), RFC2406
[4] **Douglas E.Comer.** Computer Networks and Internets, Prentice Hall, 2004
[5] **C. Huitema.** IPv6 The New Internet Protocol, Prentice Hall, New Jersey, 1996