Internet Protocol Security

N. Shahul Hameed Meeran[1] Dr. D. Venkata Subramanian[2]
[1]U.G. Student [2]Professor
[1,2] Department of Computer Science & Engineering
[1,2] Saveetha School of Engineering Saveetha University,Chennai, India.

Abstract— IP security (IP sec) is a capability that will be added to either current version of which the internet protocol (IPv4 or IPv6), it means of additional headers. IP sec encompasses three functional areas authentication, confidentiality and key management. Authentication makes use of HMAC message authentication code. Authentication mode will be applied the entire original IP packet (tunnel mode) or the entire packet except for IP header (transport mode). Confidentiality provided by an encryption format known as encapsulating security payload. Both tunnel and transport modes will be accommodated. IPsec defines a number of methods for key management.

Key words: Internet Protocol, HMAC, Cryptography, IPV4, IPV6.

I. INTRODUCTION

Internet Protocol Security (IPsec) is a protocol which suite for securing Internet Protocol. Internet protocol communications is by authenticating and encrypting foreach IP packet of a data stream. IPsec also includes in this protocols for establishing the mutual authentication between the agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway However, users have some security concerns that cut across protocol layers. For example, an enterprise can run a secure, private TCP/IP network by disallowing links to un trusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premises. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security ignorant applications

II. IP SECURITY ARCHITECTURE

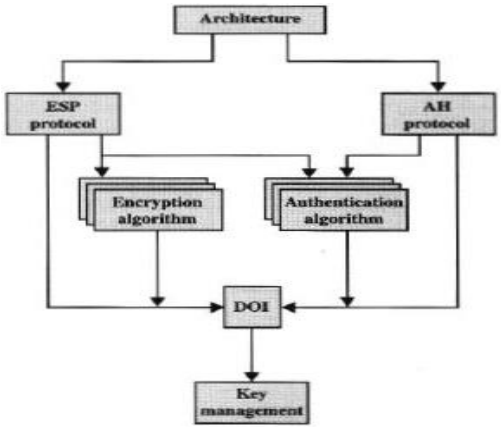

Fig.1: IP Security Architecture

- Architecture: Covers the general concepts, security requirements, definitions and mechanisms defining IPsec technology
- EncapsulatingSecurity Payload(ESP):Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally ,authentication
- Authentic Header(AH):Covers the packet format and general issues related to the use of the AH for packet authentication
- Encryption Algorithm:A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.
- Key Management: Documents that describe key managements schemes.
- Domain of Interpretation (DOI): Contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms , as well as operational parameters such as key lifetime.

A. Authentication Header:

The authentication header provides support for data integrity and authentication of IP packets. The data integrity feature ensures that undetected modification to the content of a packet in transit is not possible. the user or application and filter traffic accordingly; it also prevents the address Internet. The AH also guards against the replay attack described later.

IPsec Authentication Header

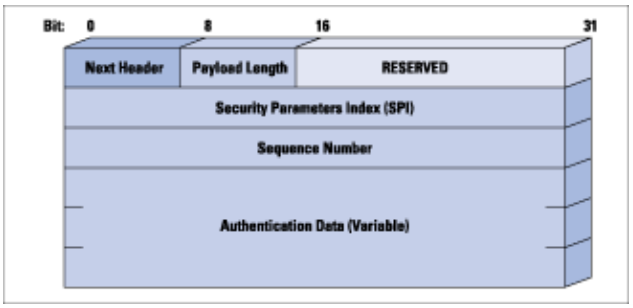

Fig. 2: Authentication Header

Authentication is based on the use of a *Message Authentication Code* (MAC);

- Next Header (8 bits): This field identifies the type of header immediately following this header.
- Payload Length (8 bits): This field gives the length of the authentication header in 32-bit words, minus 2.the Payload Length field has a value of 4.
- Reserved (16 bits): This field is reserved for future use.

- Security Parameters Index (32 bits): This field identifies a security association.
- Sequence Number (32 bits): This field contains a monotonically increasing counter value.
- Authentication Data (variable): This variable-length field (must be an integral number of 32-bit words) contains the *Integrity Check Value* (ICV), or MAC, for this packet.

B. Encapsulating Security Payload:

The encapsulating security payload provides confidentiality service, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide the same authentication services as AH.

IPsec ESP Format

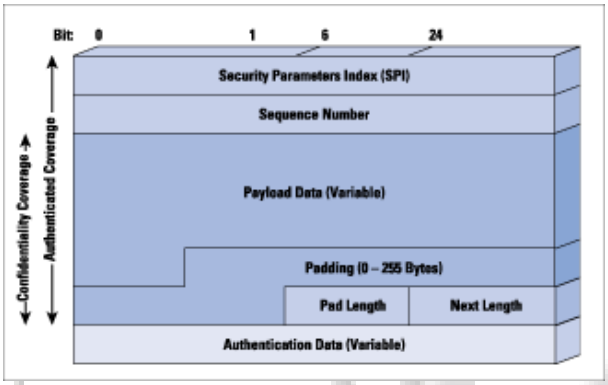

Fig. 3: ESP Format

Figure shows the format of an ESP packet. It contains the following fields:

- Security Parameters Index (32bits): Identifies a security association
- Sequence Number (32 bits): A monotonically increasing counter value.
- Payload Data (variable): A transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- Padding (0-255 bytes): Extra bytes that may be required if the encryption algorithm requires the plaintext to be a multiple of some number of octets
- Pad Length (8 bits): Indicates the number of pad bytes immediately preceding this field
- Next Header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP)
- Authentication Data (variable): A variable-length field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data field

C. Transport and Tunnel Modes:

Both AH and ESP support two modes of use: transport and tunnel mode.

D. Transport Mode:

Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Examples include a TCP or UDP segment, or an *Internet Control Message Protocol* (ICMP) packet, all of which operate directly above IP in a host protocol stack. When aESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH in transport mode authenticates the IP payload and selected portions of the IP header.

E. Tunnel Mode

Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of the new outer IP packet with a new outer IP header. The entire original or inner packet travels through a tunnel from one point of an IP network to another no routers along the way are able to examine the inner IP header .because the original packet is encapsulated the new larger packet may not have totally different source and destination address adding to the security ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header. AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

III. .KEY MANAGEMENT

The key management portion of IPsec involves the determination and distribution of the secret keys. A typical requirement is four keys for communication between two applications: transmit and receive pairs for both AH and ESP. The IPsec architecture document mandates support for two types of key management.

A. Manual:

A system administrator manually configure each system with its own keys and with the keys of the other communicating systems. This is practically for small, relatively static environments.

B. Automated:

An automated system enables the on demand creation of keys for SAs and facilities the use of keys in a large distributed system with an evolving configuration.

C. Benefits of Ipsec:

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is resistant to bypass all traffic from outside must use IP, and the firewall is the only means of entrance from the internet into the organization
- IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual sub network within an organization for sensitive applications.
- IPsec is transparent to end users and it is below transport layer so that it is transparent from applications

D. Applications of IPSEC:

- Secure branch office connectivity over internet**:** A company can build a secure virtual private network over the network or over a public WAN .this

enables a business to rely heavily on the internet and reduce its need for private networks, saving costs and network management overhead.

– Secure remote access over the internet : an end user whose system is equipped with IP security protocols can make a local call to an internet service provider(ISP) and gain secure access to a computer network .This reduces the cost of toll charges for travelling charges for travelling employees and telecommuters

This is a typical scenario of IPSEC .An organization Maintains LANs at dispersed locations. Non-secure IP traffic is conducted on each LAN for traffic offsite, through some sort of private or public WAN, IPsec protocols are used. These protocols operate in networking devices,such as router that connect each LAN to outside world. The IPsec networking device will typically encrypt and decrypt the data. These operations are transparent to Workstations and servers on LAN.

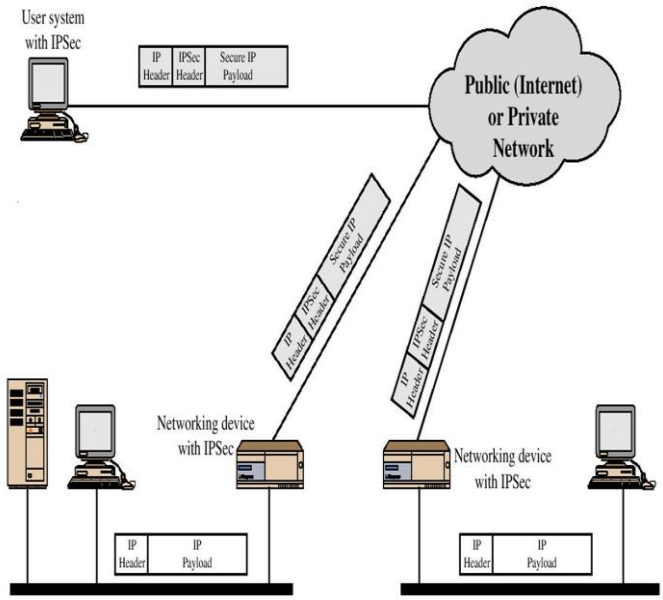

Fig. 4: Applications of IPSEC

IV. CONCLUSION

As you've seen, there are many useful things you can do with IPSec, but it is not a silver bullet for security. You need to have proper management of setting up the VPNs, and to be careful that you are not opening yourself up to problems. By allowing another network access to yours over a VPN it is important to recognize that the security policy of the remote end will affect yours.

REFERENCES

[1] Network security essential by William stallings
[2] http://en.wikipedia.org/wiki/IPsec
[3] http://www.itd.nrl.navy.mil/
[4] http://ezine.daemonnews.org/199812/security.html
[5] http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml
[6] http://support.microsoft.com/?kbid=884909
[7] http://support.microsoft.com/kb/818043/en-us
[8] http://www.microsoft.com/windows2000/technologies/communications/ipsec/default.mspx
[9] http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx
[10] http://technet.microsoft.com/en-us/network/bb531150.aspx
[11] http://technet.microsoft.com/en-us/library/cc748991%28WS.10%29.aspx
[12] http://www.safenet-inc.com/products/swTK/index.asp
[13] http://docs.sun.com/app/docs/doc/817-2694?a=expan

