CNS : IPsec Lecture

What is IPsec ?

- IPsec is a set of protocols (suite) that cooperate to secure IP communications (at the network layer and above).
- Previously with TLS we secure only the Application Layer.
- Used to setup certain VPNs (secure ones)
- provides mutual auth, integrity, confidentiality , and sometimes non-repudiation (certificates).
- Its components : **AH** (Authentication Header, to protect the header of the IP, i.e integrity, so that nobody can change the content of the IP header while transit, we are using HMAC so the attacker needs to find the key **-INTEGRITY-**), **ESP** (Encapsulating Security Protocol, to protect the header and encrypt the payload, sometimes we encrypt even the header and then add another header from the outside, i.e hiding the original IP, and this is what VPNs do **-CONFIDENTIALITY-**) and **SAs** (Security Associations, they are like contracts to tell you which encryption algorithm we gonna use, which integrity function, which key derivation function, the size of the key, the lifetime.....).

- to build the **SA**s there is a framework called the **ISAKMP (Internet Security Associations Key Management Protocol)** which is implemented using a protocol called **IKEv1** and **IKEv2.**
- from **IKEv1 to IKEv2 :** to achieve less messages with better security.
- An interesting thing in IPsec : in one traffic direction (eg, outbound) I use a set of algorithms to encrypt and ... while we can use a different set of algorithms for the inbound traffic also with a lifetime.
- **IKE** runs over **UDP 500 ,** and **UDP 4500 (NAT-traversal)** so that when the packet is Natted it doesn't get dropped due to IP change.
- IPsec aims to stop : **Eavesdropping**, **modification**, **spoofing** of datagrams, even **replay** of datagrams (it add a nonce, which has a lifetime, which can be measured by time or bytes exchange, this lifetime affects the SA by renegotiating it once nonce is expired), also **MITM** and **session Hijacking** due to encryption+ auth, also **DoS** attacks thanks to anti-spoofing and cookies(just like TCP cookies).
- IPsec supports two operational modes : **Transport**(by creating a secure channel between two hosts, here there is the problem of the HMAC with NAT, so we use NAT traversal by encapsulating the packet and decapsulation at the end) and **Tunnel(**this is the story of VPNs , using gateways , it creates a secure channel between gateways, where your original IP will be hidden encrypted (the whole packet is encapsulated once reaching the Gateway), and what is transiting in the channel is encrypted , you can only see the IPs of the gateways) modes.
- SA is a unidirectional digital contract(a data structure), stores a set of security parameters, algorithms and keys.
- two types of SA : **IKE SA** (Parent SA) and **IPsec SA** (child SA), the first is established to securely establish the second.
- structure contains :
  - id called Security parameter Index (SPI), in **IKE SA** it is 64+64 bits (half from initiator and half from responder) and in **IPsec SA** it is 32 bit .
  - a sequence number, 0⟶window, after that we have to negotiate a new SA (child SA)

    - IP protocols in use.
    - Encryption also for ESP, propose and select.
    - Integrity/hashing algo
    - encryption and message authentication keys
    - operational mode
    - lifetime
    - traffic selector (IP address range, port range, protocol....)
- in the terminology of IPsec : Responder-Initiator is server-client.

ISAKMP Phases:

IKEv1 :

two main phases :

- **Main Mode** : exchange 6 packets, in message 1 (M1) initiator sends SPI and nonce and proposed algorithms, in message 2 responder sends same and select algorithms from the proposed ones, in M3 and M4 they exchange DH with a nonce to derive key, which is a seed along with the agreed upon PRF (Pseudo Random Function) and nonces to derive a set of 3 keys :one for encryption , one for auth and one to be a seed to the Child SA, then M5 , M6 are encrypted to exchange the IDs and auth proofs, **hence IKE SA is created now.**
- **Quick Mode :** establishing the Child SA which is encrypted phase by exchange 3 packets, M7 and M8 are for renegotiating the protocols, M9 initiator confirms by a hash on M7 and M8.

IKEv2 :

two main phases :

- **INIT phase** : exchange 2 packets (IKE-SA-INIT req and IKE-SA-INIT response), to exchange SPI and nonce and proposed algorithms along with [DH public value].SPIs are combined into 128-bit SPI. key is derived, which is a seed along with the agreed upon PRF (Pseudo Random Function) and nonces to derive a set of 3 keys :one for encryption , one for auth and one to be a seed to the Child SA, **hence IKE SA is created now.**

- **AUTH phase :** establishing the Child SA which is encrypted phase by exchange 2 packets (IKE-AUTH req and IKE-AUTH response), no protocols renegotiation , exchanging the IDs and auth proofs with certificates ,a signature over the IKE-INIT message or hash with PSK… The IPsec SA is made of two unidirectional Child SAs (one for each traffic direction inbound and outbound), each with its own SPI (Security Parameter Index) and independent cryptographic parameters (algorithms & keys).

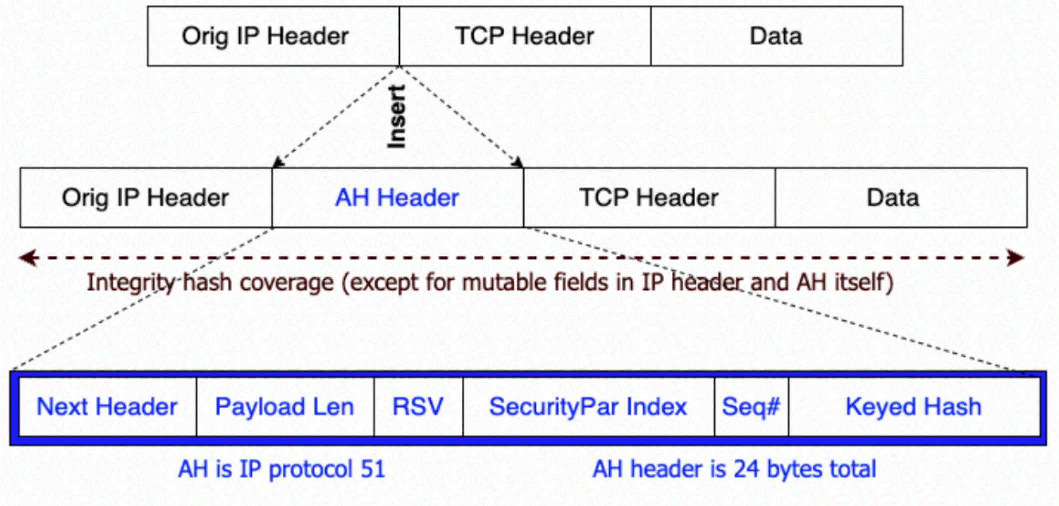
> When the Encryption algorithm is : **AES-GCM** no need to specify a hash function , because this encryption algorithm (with Galoi Cyclic Mode) it preforms encryption and integrity. which is not the case when using **AES-CTR.**

> To be able to decrypt the IP datagrams, first find the Parent SA, once decrypt it, find Child SAs, then you can decrypt…

IPSec: Protection with AH and ESP

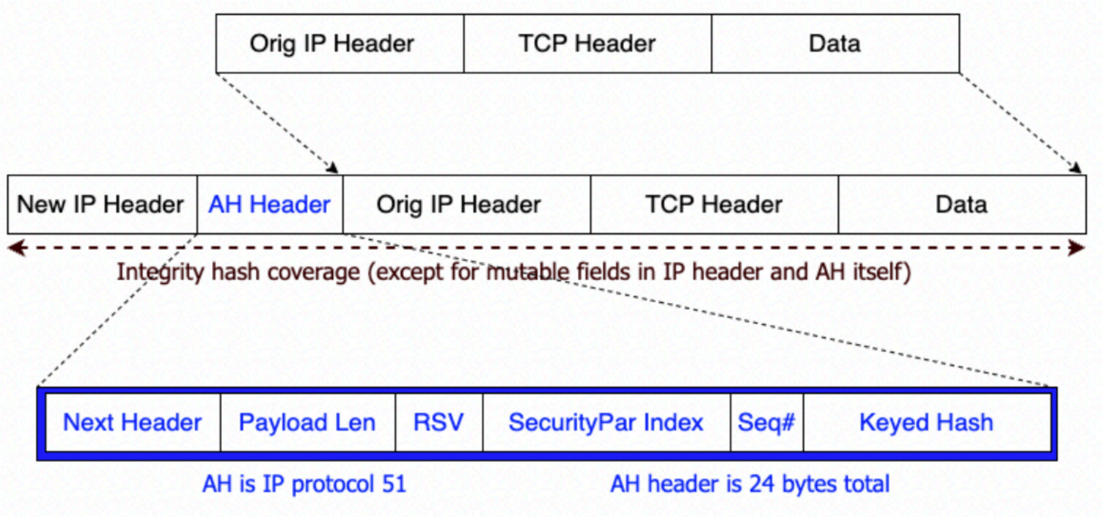
Authentication Header (AH):

It guarantees data origin authentication, data freshness, and data integrity. It does not ensure data confidentiality.



AH header in transport mode

- We perform the integrity hash on the whole datagram, the AH Header will be considered NULL, and some mutable fields are set to 0 ,like TTL.
- Next Header tells which protocol is next.
- Payload length : length of the AH Header, it is variable depending on the used hash function.
- Seq# to prevent Replay.
- SPI to know which SA is used to decrypt...

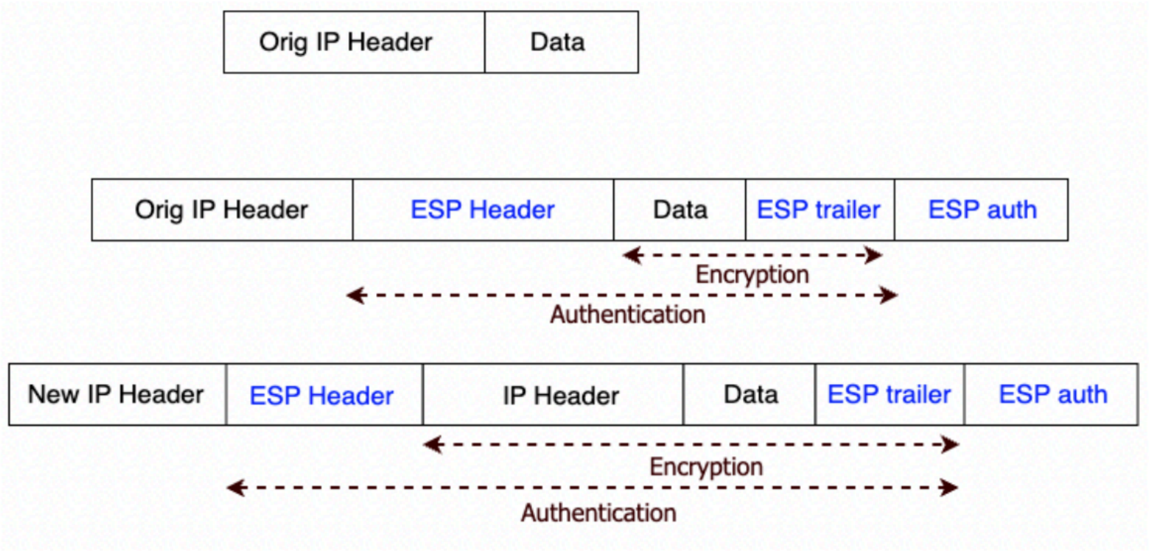


AH header in tunnel mode

- new IP header is for the Gateway.
- We perform the integrity hash and authentication on the whole datagram, and we care about the Gateway header, bcz there was an attack called CUT&PASTE by cutting the the packet from new IP header which will be replaced by a spoofed one, which my take another route.
- Intigrity check value (multiple of 32 bits in IPv4): HMAC value.

Encapsulating Security Payload (ESP)

It provides origin authenticity through source authentication, data integrity through hash functions and confidentiality through encryption protection for IP packets.



ESP header in both modes.

The interpretation of ESP information fields is as follows:

- ESP header: consists of:
  - Security parameter index (32 bits) — (which SA to use here).
  - Sequence number (32 bits) for packets freshness.
- ESP trailer:
  - Padding (0-255 bytes).
  - Padding length (8 bits).
  - Next header (8 bits).
- ESP Auth: Integrity check value, a multiple of 32 bits.

> Not all VPNs use IPsec. There are several other VPN technologies, each
>
> with different use cases. E.g., TLS-based VPNs (OpenVPN, AnyCon-

> nect, etc) provide encryption of application-layer payload only.

IKEv2 is more efficient, secure, and modern than IKEv1, with fewer exchanges, mandatory PFS, and better support for mobility and rekeying:

- IKEv1 and IKEv2 are not interoperable.
- IKEv1 uses 9 messages, whereas IKEv2 uses 3.
- IKEv2 has DoS protection built-in (using cookie).
- IKEv2 has anti-replay protection mandatory.
- IKEv1 re-negociates SA during Phase 2.
- IKEv2 has perfect forward secrecy (new DH for each child SA).
- IKEv1-PSK (aggressive mode) is weaker than IKEv2-PSK.
- IKEv2 natively supports ECDH groups.
- IKEv2 supports mobility (MOBIKE).