Important Protocols

IpSec

What is IpSec?

RFC 6071(IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap)

IPsec is a protocol that provides a secure tunnel between two computers. It is used to protect data that is transmitted over the internet.

IPsec helps mitigation against:

- eavesdropping
- theft
- replay attacks,
- Data corruption.

Ipsec operates in 2 different modes: tunnel mode and transport mode.

In ***tunnel mode***, everything is encapsulated in IPsec datagram. when data is transmitted, the layer 3 devices only use IPsec header to route the packet.

This is used basically in the site-to-site VPN and remote access VPN.

in ***transport mode***, all of the data is protected but the original IP header is not. Payload is protected by IPsec. This is used generally in P2P applications.

Ipsec building Blocks:

Ipsec Suite either uses **Authentication Header(AH)** or **Encapsulating Security Payload (ESP)**. One difference is that in the former, the data is encrypted.

ESP and AH both come with options of transport and tunnel.

In the AH transport mode, the payload is encrypted and the original IP header is not protected. In the tunnel mode, the payload is encrypted and the original IP header is protected. A new IP header is appointed to the packet in tunnel mode.

ESP transport and Tunnel modes can be used as it is or with AH.

ESP enapsulates the data so we have both header and trailer in the packet in Transport mode and in Tunnel mode.

in ESP header, different than AH header, there is no next header field and payload length field.

Afther the headers, there is `Security Association (SA)`.

Security Association in IPsec suite is a `unidirectional connection` that gives devices the capability to use AH or ESP services. for a bidirectional comms, a pair of SA is needed.

In order SA to be established, the following steps are needed:

- **SPI**: Security Parameter Index. It is a unique number that is used to identify the SA.
- **Security Protocol Identifier**: It is a number that identifies the protocol that is used in the SA. (50 for AH or 51 for ESP)
- **Destination IP Address**

For key management, it is either done manually or automated using IKEv1 or IKEv2.

IKE (Internet Key Exchange) is a protocol that is used to establish a key management between two computers. default one is IKEv2.

Next building block is **Crypto Algorithm**. These are used for Encryption , Authentication , Integrity and Pseudorandom Number Generation.

====

for SA estabblishement, there are couple of different protocols that are used.

- ISAKMP (Internet Security Association Key Management Protocol) : Used for procedures and formats to establish SA. It helps us build the SA.
- OAKLEY (One-Way Authentication Key Exchange Protocol) : gives key-exchange mechanissm. Used to exchange key over insecure connection using Diffie-Hellman.
- SKEME (Security Key Exchange Method) :gives anonimity and reputability through key-exchange techniques.
- IKE (Internet Key Exchange) : Uses combination of ISAKMP, OAKLEY, and SKEME

=========

Ipsec in Enterprise

In enterprise level, there are 2 main uses of IPsec:

- Site-to-Site VPN

connect 2 or more sites together. One type of Site-to-Site VPN is `DMVPN` (Dynamic Multicast VPN).

`logically` connects sites, protects `entire` network, provides corporate resources to other sites.

- Remote Access VPN

`logically` connect endpoint to another network. IPsec using the OS IP stack. protects `individual` devices.

useful in wifi hotspots.

Bu mesela bir isci evden calisirken isyerinin agina ulassin diye kullanilan vpn. ticari bireysel VPNler de bu tip, hotspotshield, NordVPN gibi.

as for IPsec implementations, there are 2 main types:

- GRE over IPSec

way more commen.

encapsulates entire packet. this is essentially DMVPN over IPSec.

- IPSec over GRE

much less common. only the payload is protected via IPsec. routing information stays visible in the GRE portion of the datagram.

IKEv2

What is IKE?

IKE is Intrnet Key Exchange that uses ISAKMP, OAKLEY, and SKEME for establishing SA for securing network traffic.

Although IKEv1 is still used, IKEv2 is the new standard and IKEv1 is obsolete.

V2 brought these:

- new authentication method EAP (Extensible Authentication Protocol) alongside PKS and PKI
- brought MOBIKE (Multicast Opportunistic Key Exchange) which allows dynamically change IP adresses without needing to re-establish the SA.
- in V1, SA lifetime was negotiated, in V2, SA lifetime is configured locally and faster negotiation.
- Flexible traffic selection per SA.

Some benefits of IKEv2 are:

- **It is more reliable:**

message flow system uses requests followed by responses. Initiator sends a request, and the responder sends a response. If the initiator does not receive a response, it will retry or drops the request. the reliability is on the initiator side.

- **It is more Mobile:**

using MOBIKE, keeps VPN conenction active when changing IP addresses. thanks to `multihoming`, when interface drops, the traffic is moved to another interface.

- **it enables `High Availability`:**

IKEv2 comes with `redirection` feature. if one server for VPN is taken down or went down, the users can be redirected to another server.

For authentication, IKEv2 uses `Pre-Shared Key` (PSK) and `Certificate Authentication`. Apart from that uses EAP.

==========

MacSec

Macsec is defined in 802.1AE as `point2point security protocol` providing `data confidentialiity, integrity, and origin authenticity` (all CIA triad.) for traffic over LAyer 1 or Layer 2 links and is part of larger security ecosystem.

Technically, on the transmit side of the link,MAcsec adds `Mac Security Tag` (SecTag, 8 to 16 bytes) and `Integrity Check Value` (ICV, 8 to 16 bytes) to the packet and can optionally encrypt the packet. on the receive side of the link the MacSec engine can identify and decrypt the packet, check integrity, provide `replay protection` and remoce SecTag and ICV. Invalid frames are discarded or monitored.

There is a need to protec data that is transmitted over the in-vehicle ethernet that is connecting `ECU`s together.

Data security protocols like MacSec are often deployed in Ethernet Local Area Networks(LAN) that support `mission critical applications`.

Macsec prt the `IEEE 802.1AE` standard PREVENTS LAYER 2 SECURITY THREATS SUCH AS PASSIVE WIRETAPPING, INTRUSION, MITM, AND REPLAY ATTACKS BY OFFERING LINE-RATE ENCRYPTION AND PROTECTION OF TRAFFIC LASSING OVER LAYER 1 AND/OR LAYER 2 LINKS.

Although it is desirable, it is **not practical to secure the entire network against physical access** by determined attackers. **Macsec allows only authorized systems that attach to and interconnect LANs in a network** to maintain confidentiality and integrity of data and take measures against data theft.

- **Where does Macsec fit within OSI-layer model?**

On the layer 1, there is Automotive Ethernet Physical Layer (AEPL) which is the layer that connects the physical layer of the vehicle to the network. these are like 100baseT, 1000baseT etc.

On the next layer, which is Layer 2, there is IEEE Ethernet MAc + VLAN(802.1Q) + AVB(802.1Qav) + TSN + `MacSec`. Hence, macsec is a layer 2 protocol that is sitting on top of the bare metal.

On the layer 3, there is IPv4 and IPv6 which are protected by `IpSec`. Hence IpSec is a layer 3 protocol.

- **What are some common Security Threats?**

These are some of the common threats against Ethernet Lan:

- Eavesdropping (compromising routers, links, DNS, or algorithms)
- Sending arbitrary data including IP headers.
- Replay attacks.
- Tampering message in transit.
- writing malicious code and deceiving people into running it.
- exploiting bugs in software to take over machines ans use them as base for future attacks.

While IPsec is encryption at Layer 3, MacSec is encryption at Layer 2 which is Ethernet layer.

Remember this : ==> `IEEE 802.1AE`

Compared to IPsec:

- MacSec provides STRONGER ENCRYPTION performance at HIGHER SPEEDS.
- Macsec can encrypt user data at UP TO 800Gig Ethernet Speeds without any hardware offloading.
- Application to any network that relies on Ethernet so can be used in many places => so Data Center, Corporate environment, Service Provider, etc.

Packet Structure:

A captured MacSec packet has some options and payloads.

-> **802.1AE Security Tag.**

This Tag has some option flags like VER, ES, E.

E flag is set to 1 if the packet is `encrypted`.

-> **ICV Value**

ICV is a checksum that is used to verify the integrity of the packet.

-> **Port Identifier.**

shows on what port the packet was captured on.

-> **Data**

Data is the encrypted payload. looks like a random hash value.

MacSec Terminology:

1. **MacSec Key Agreement Protocol**

Used to discover Macsec capable peers and used to negotiate encryption keys. These keys are for `data encryption` and `Security Associataion Key Encryption`(SAK)

2. **Connectivity Association (CA)**

Similar to `IPSec SA` but for MacSec. Defines a secure relationship between MacSec peers.

3. **Connectivity Association Key(CAK) **

Static or Dynamic Key exchanged by macsec speakers. This can be seen as `primary key` that is used to device all other session keys.

So CAK is used to derive SAK keys and this SAK keys are used to encrypt the user data.

So this CAK can be statically confiugred or can be distributed by the server.

4. **Connectivity Association Key Name (CKN) **

Any name that defines a CAK.

5. **Primary and Fallback Keys **

Primary key is used to negotiate an MKA if this fails, Fallback key is used.

6. ** Security Association Keys(SAK)**

Derived from CAK used to encrypt data as mentioned earlier.

A `Key Server` generates SAK. If you have if you have one switch connected to another switch on ethernet link and MacSec is enabled on this switch, one of these switches will be a Key Server. You can either configure one of these switches as higher priority to make it key server

if you enable MacSec on an interface, it drops all frames except MAcsec encrypted frames. But you can configure macsec profile to allow unprotected traffic in macsec negotiation fails.

==========

ArpSec