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.
- Very little latency.
- Application to any network that relies on Ethernet so can be used in many places => so Data Center, Corporate environment, Service Provider, etc.
- Allows to protect all protocols virtually, including layer 2 protocols like AVB TP (IEEE 1722)
- The smallest attack surface on Ethernet-based links for attacks with physical access to a medium

IPSEC and TLS are software based but MacSec is hardware(phy and switches) based. so it makes it more robust and secure!

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.

After authentication and key exchange are performed, a secure communication link, called `Secure Channel` is established using Macsec from one node inside CA to another. in MAcSec protected network,

each node has at least one `unidirectional secure channel`. The Secure channel does not expire and lasts for the duration of the communication between two nodes. Each secure channel is associated with an `identifier` : the `Secure Channel Identifier` SCI.

Within each secure channel(both transmit and receive), Secure Associations are defined. each Secure association has a corresponding `Secure Association Key` (SAK) and is identified by the Association Number field of the SecTag header. Secure Associations have limited duratuion. this is called Key Rotation.

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.

Within each Secure Association, `replay protection` can be performetd by checking the Packet Number field of SecTAG header agaisnt the packer number locally stored since ehac macsec packet has a uniqe sequential packet and each packet number can be used only once.

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.

====================**==========**==========**==========**

What is IEEE 802.1X

IEEE 802.1X is a network authentication protocol that opens ports for network access when a user's identity is authenticated it also authorizes them for acess to the network.

IEEE 802.1X is an Port-Based Network Access Control(PNAC) standard that provides protected authentication for secure network access.

an 802.1X network is `different from home networks in one MAJOR way`: it has an authntication server called `RADIUS Server` which checks user's credentials to see if they are an active member of the organization and , depending on the netwrk policies, ggrants them various access rights. This helps unique

credential creation for each user, eliminating the reliance on single network password that can be easily cracked or stolen.

the RADIUS server is able to do it in various ways, typically over LDAP or SAML protocol.

What are possible MACsec use cases within Ethernet Network

If a hacker taps into the macsec disabled network, the flowing data can be obtained by hacker and can be used to perform attacks. Hacker can target switches, can tap into the network, or can monitor the device.

if macsec is enabled, tapping or eavesdropping, or replay attacks are not possible since packets are numbered, encrypted. **HOWEVER** hacker CAN disrupt the network using DOS attack if DOS prevention is disabled. in this case, neither hacker nor the vehicle can receive the packets. if DOS prevention is Enabled, the Video stream(i.e.) remains disturbed but DOS does not propogate through the Ethernet phy.

Macsec is cost-effective and could be used in combination with other technologies like IPsec, TLS, etc.

ArpSec

CyberSecurity Notes

ISO/SAE 21434

==> Automotive Cybersecurity standarts are defined by `ISO/SAE 21434`

Helped creating common terminology accross the industry.

Helped creating minimum base criteria for cybersecurity in the vehicle.

Creating security assurance level.

It is a reference that regulators point to. In order to enforce a standard, now regulators have a reference point.

The scope of ISO 21424 :

- Risk Management (Assess, monitor, evaluate potential risks.)
- Product Development (security of systems, hardware&software,
- performing TARA(Threat Analysis Risk Assessment))
- VARA (vulnerability analysis risk assessment)
- Operation, maintenance, and processess. Starting from beginning to the end, covers all aspects.
- process overview and interdepencencies.
- An `Assurance Level` is defined with ISO 21424 which is `Cybersecurity Assurance Level` this is like common security assurance level like how secure is the system or how much trust you can put onto it.

CanBus IDS/IPS vs Ethernet IPS/IDS

Comparing Can and Ethernet

CanBus is a Bus topology which means when a message leaves and ECU, it is guaranteed to reach any neighbir ecu on the same bus. Meaning there is no way to stop an attack using software which reside in the gateway since it is just listening to the traffic. Gateway can only stop propogation of the message from one bus to another but not on the same bus.

On the other hand, the ethernet is a star topology meaning on each port there is exactly one device is connected any device that is sent by the device can be inspected by the gateway.

Since ethernet is MUCH more speedy comparing to the Can, any IDS or IPS system needs lots of horsepower to be able to undertake full or partial analysis.

Message length in Can bus is only 8 bytes (60 for Can FD) compared to Ethernet which is 1500 bytes.

In terms of `source identification`, there is no source ID in can bus there is only Message ID. So you cannot tell who sent the message. This can be done using encapsulated protocols like `j1939` but standard does not have message origin identification. Can bus does not have any specific `message destionation` as well, it only has `message id` which is a `multicast` address that anyone can listen to it.

In ethernet, on the other hand, there is `distinct unicast` that means it has source and destination mac addresses, all clear. and etherenet support both unicast and multicast hence, with ethernet it is much easier to detect the source of a message.

Beware that `automotive ethernet` is not necessarily about ethernet, it is about all the networking. For example, on top of ethernet sits MAC, and then on top of that sits IP, on top of that sits TCP/IP or UDP/IP. To the application level, there is DoIP.

Can and Autmotive Ethernet IDS/IPS work process

IDS/IPS is designed to counter an attacker manipulating network traffic via a malicious application, hacked ECU or other controller.

It has 3 steps:

- It `learns` the normal.
- it `monitors` the network traffic and the `Routing` function of gateway rules
- it `Detects` anomalies based on deviation from `normal`. Prevents by discarding frames when possible.

Comparing CAn and Ethernet Rules Generation

- both of the them require recordings to generate rules out of it.
- Both of them use `files` where CAN uses DBC extension, ethernet uses XML.
- Both of them allow user to edit rules manually.

- Rule generation is simple in CAn Bus(but can get complicated if j1939 is used) and is complex in ethernet due to network nature (Mac adresses, DHCP, DoIO etc protocols)
- CAN is static, predictive and deterministic and uses whitelisting. But ethernet is more volatile, it uses both black and white lists simultaneously, also `signature based` detection. Signature based detection is not implemented in Can Bus.

CAN and Ethernet IDS/IPS Architecture

IDS systems are essentially sdk integrated into ecu. This ECU can be an existing ECU like gateway or a dedicated ECU attached to CAN bus.

Incoming message/frame is `routed` to IDS/IPS to be processed.

the IDS/IPS inspects the message/frame and returns its findings with the associated information.

In case of anomaly, an event is reported.

when configured as IPS, when possible, the anomalous packet is discarded.

Canbus:

In Canbus, these IDPS will most likely be integrated into gateway, in other cases, it can be connected directly into ecus.

If we use IDS not IPS, it just taps into network so there is no need for changes in the vehicle.

Ethernet:

it `definitely` goes into gateway. it serves as automotive backbone.

Message Formality

Canbus:

Relatively easy to validate the format since the message is very short. only exception is CanBus TP(transport protocol) and SAE j1939 TP is used which adds more complexity.

Ethernet:

Etherned side of the message is much harded, needs 7 layer `Deep Packet Inspection(DPI)` to determine individual message format validity. For example:

- Ethernet frame
- IP header
- UDP header
- DoIP PDU header
- UDS PDU header