MARVELL

White Paper

The Need for MACsec Security in Ethernet-Based Vehicle E/E Architecture

November 2020

Content

1.0 Introduction to MACsec in the Automotive E/E Architecture

As Ethernet becomes an essential part of the overall Automotive E/E Architecture for connectivity between Electronic Control Units (ECUs) within the Vehicle platform, the need arises to protect the data that is transported on such connectivity links.

Data security protocols, such as MACsec, are often deployed in Ethernet Local Area Networks (LANs) that support mission-critical applications. Historically these have included corporate networks of considerable extent and public networks that support many customers with different economic interests.

MACsec per the IEEE 802.1AE standard prevents Layer 2 security threats, such as passive wiretapping, intrusion, man-in-the-middle and playback attacks by offering line-rate encryption and protection of traffic passing over Layer 1 and/or Layer 2 links.

Preventing disruption and data loss arising from transmission and reception by unauthorized parties is highly desirable, since it is not practical to secure the entire network against physical access by determined attackers. MACsec allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against data theft.

The scope of the MACsec standard is to provide the following:

- Origin of Data – to ensure the frame was sent by MACsec peers
- Connectionless authenticity – to ensure that the frames have not been modified en route
- Confidentiality – the encryption of the frame's EtherType and content of payload to ensure that they cannot be read en route
- Replay Protection – to ensure that the same frame is not received more than once.

The figure below highlights where MACsec security fits within Layer 2 of the overall Ethernet OSI 7-layer model, which has been adopted within the IT Standard and incorporated into the Automotive E/E Architecture ecosystem.

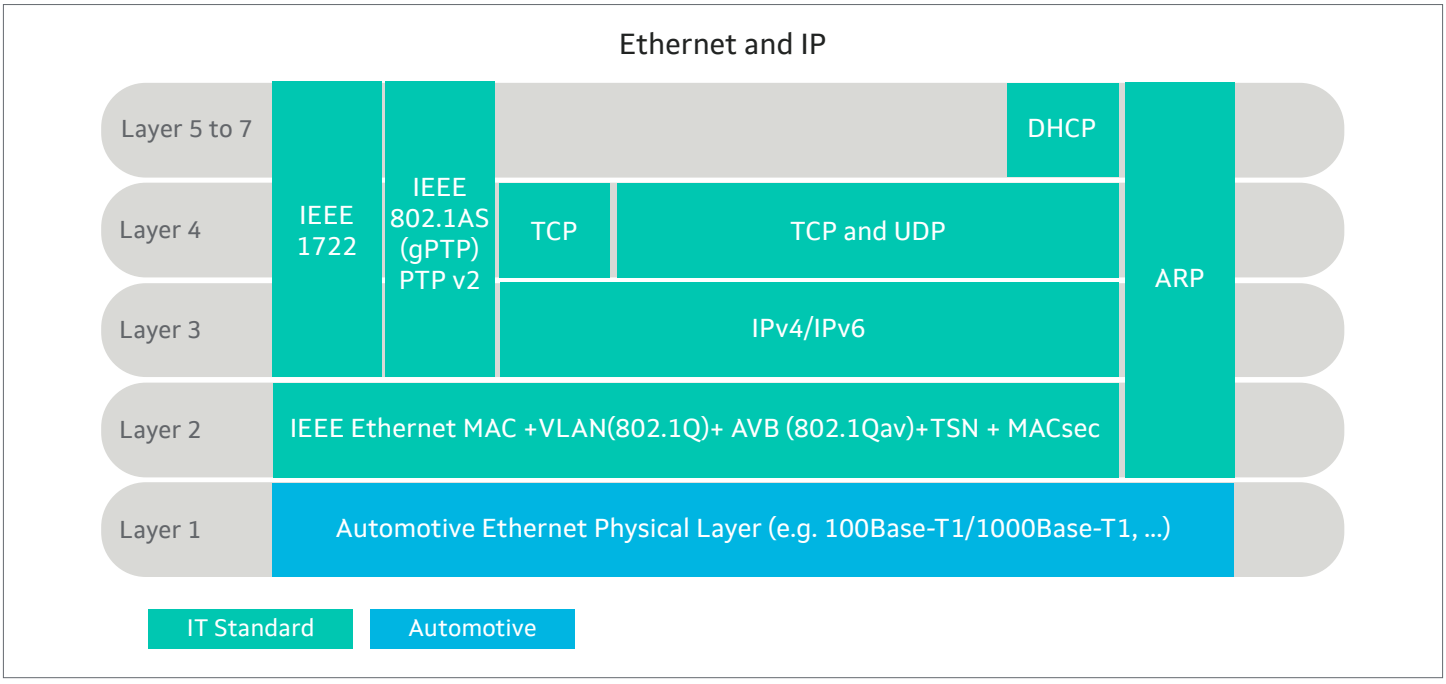

Figure 1: Ethernet OSI 7-layer Model

**Ref: Comparing Automotive Network Security for different communication Technologies - Dr. Lars Völker.*

2.0 Common Security Threats

Some of the security threats intruders can carry out in Ethernet LANs include, but are not limited to:

- Eavesdropping (compromising routers, links, routing algorithms, or DNS)
- Sending arbitrary messages (including IP headers)
- Replaying recorded messages
- Modifying messages in transit
- Writing malicious code and deceiving people into running it
- Exploiting bugs in software to take over machines and use them as a base for future attacks

3.0 What is MACsec?

MACsec stands for Media Access Control Security or MAC Security and is defined in IEEE 802.1AE as a point-to-point security protocol providing data confidentiality, integrity and origin authenticity for traffic over Layer 1 or Layer 2 links and is part of a larger security ecosystem for Ethernet LANs. On the transmit side of the link, MACsec adds MAC Security TAG (SecTAG) and ICV (Integrity Check Value) to packets and can optionally encrypt the payload. On the receive side of the link, the MACsec engine can identify and decrypt the packets, check integrity, provide replay protection and remove SecTAG/ICV. Invalid frames are discarded or monitored.

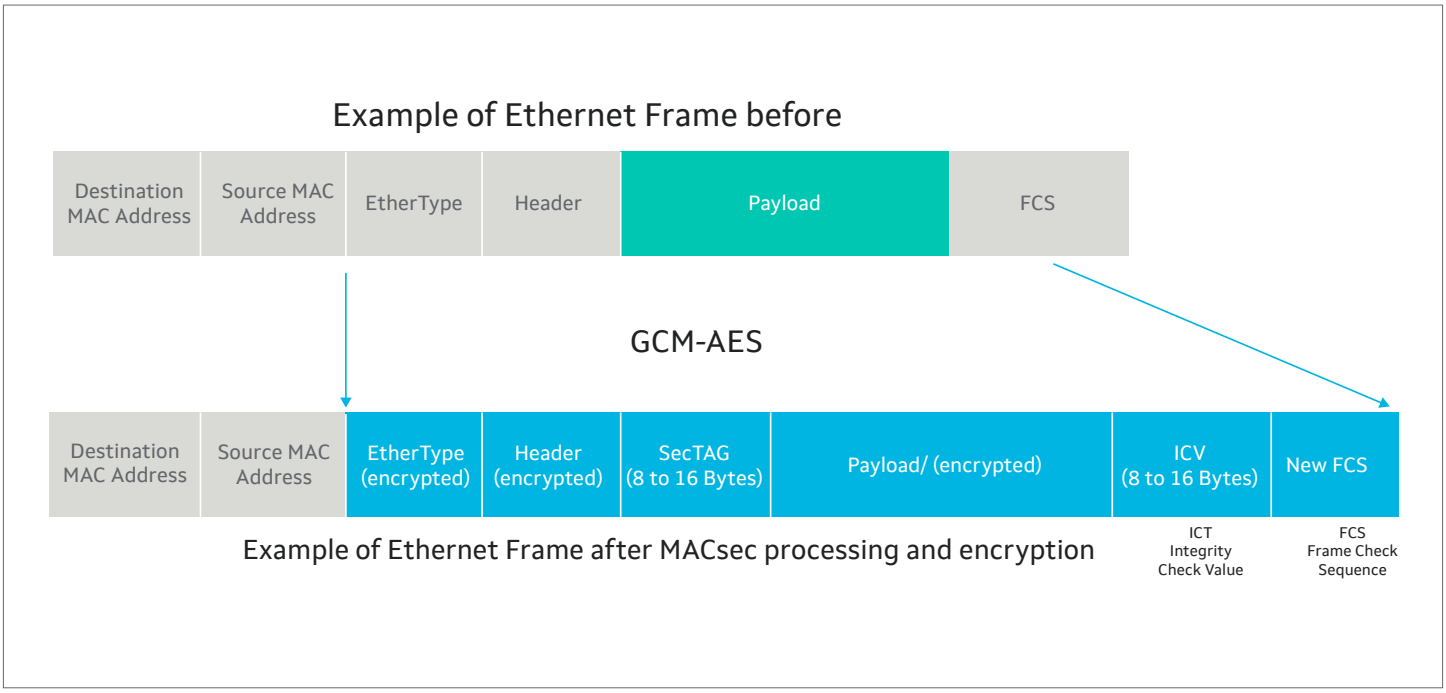

Figure 2: Ethernet Frame before and after MACsec processing and encryption.

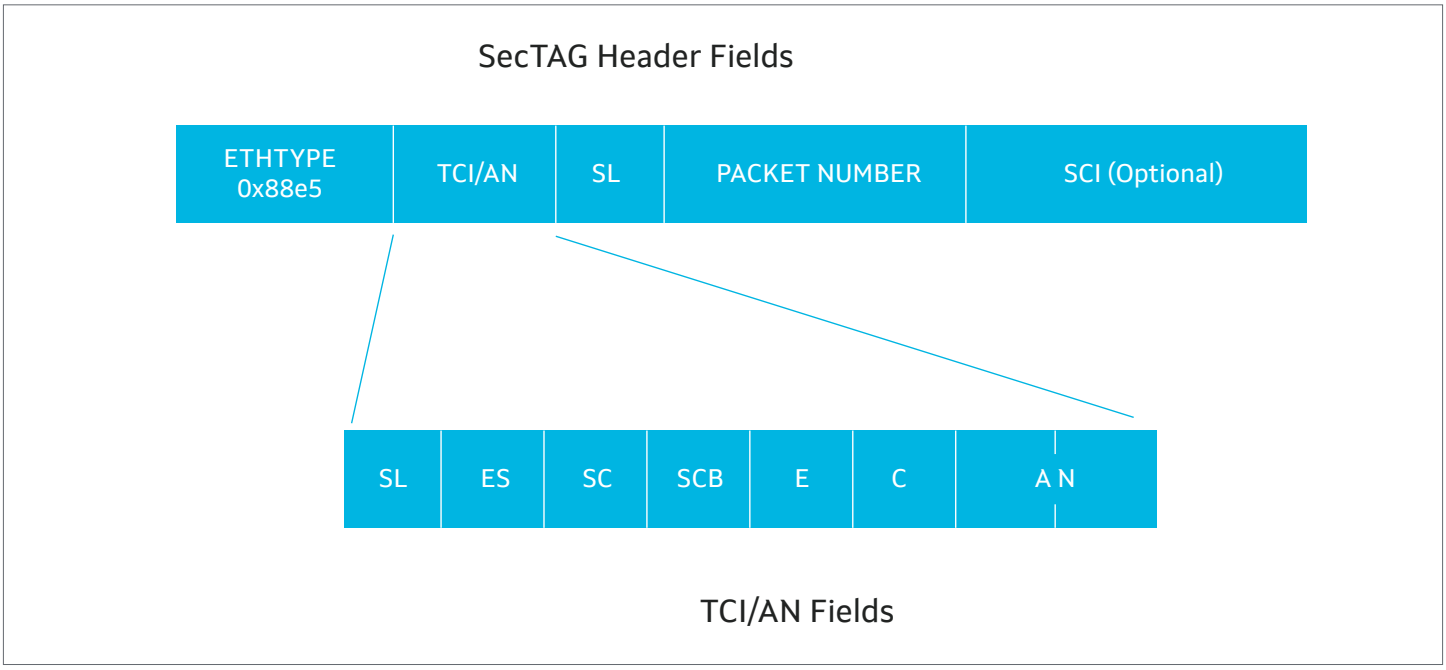

Figure 3: Content of SecTAG Header Fields.

**Ref: MACsec: a different solution to encrypt network traffic - Red Hat Developer*

- V (version) is always 0
- ES is End Station bit
- if SC is 1, SCI field is present (16-byte header)
- SCB is Single Copy Broadcast
- E and C bits used to determine if packet is encrypted
- E, C = 1, 1 – Encrypted
- E, C = 0, 0 – Authenticated-Only
- AN used for key rotation

MACsec works at the device level and the following are some of the key functions of MACsec:

**Ref: 8021AE-2018*

Data Origin Authenticity:

It can be determined if packets originated from authenticated link partners, or not, by checking the SecTAG.

Integrity Check:

The integrity of frame content is verified upon receipt. Whether packet contents have been modified in transit, or not, can be determined by checking the ICV.

Encryption:

For confidentiality purposes, data transported within the MACsec-protected link (Secure Channel) can be optionally encrypted and decrypted using an industry-standard GCM-AES-128 or 256 cipher suite. Payload of the packet that comes after SecTAG can be encrypted. This is done per GCM-AES and provides a guarantee that only the nodes which possess the symmetric key can decrypt the packets.

Replay Protection:
Authentication/Authorization and Key Management/Exchange:

Authenticating and authorizing/denying devices attached to the secure LAN and key exchange/management between link partners, etc., are covered by IEEE 802.1X. Possession of a symmetric key is regarded as proof that a device has been authenticated and ready to start MACsec sessions.

Although MACsec/802.1AE does not directly perform the above functions addressed by 802.1X, it does assist in the following ways:

- MACsec enforces prior authentication
  - Traffic will not be received without a valid symmetric key
  - Traffic received on an invalid key will be discarded
  - The only way to get a key is through authentication
- MACsec makes Denial-of-Service Attacks difficult
  - Although MACsec cannot prevent a device from transmitting, it can prevent a device from lying about its identity (e.g., MAC address)

4.0 Architecture of MACsec

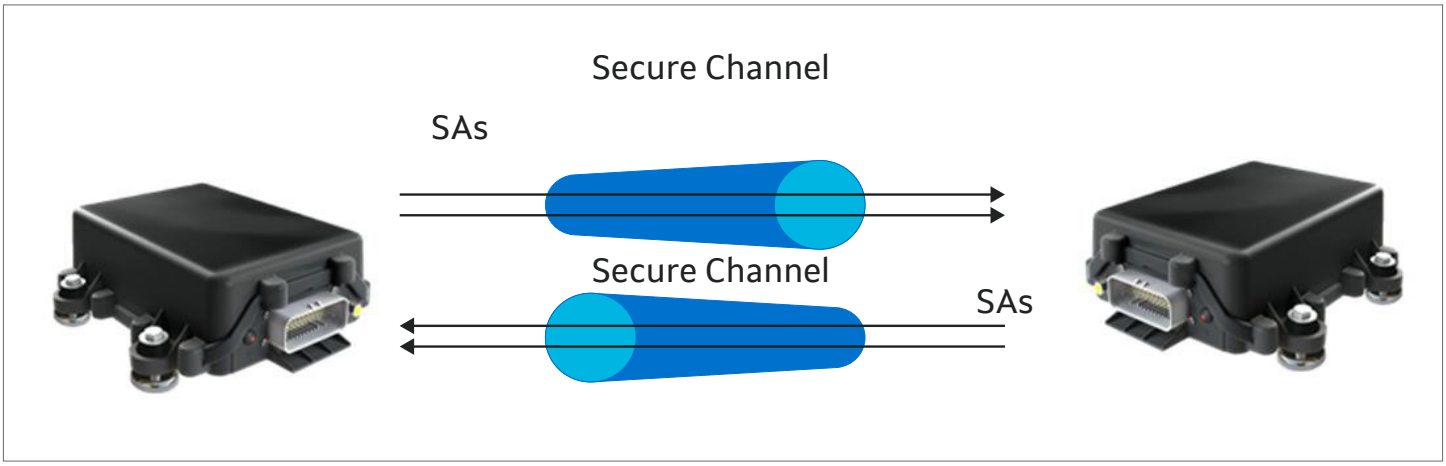

Figure 4: Establishment of Unidirectional Secure Channels.

Secure Channel:

After authentication and key exchange are performed per the IEEE 802.1X standard, a secure communication link, called a Secure Channel, can be established using MACsec from one node inside the Connectivity Association to another. In a MACsec-protected network, each node has at least one unidirectional secure channel (transmitter to receiver.) The Secure Channel does not expire and lasts for the duration of communication between two nodes. Each secure channel is associated with an identifier: the Secure Channel Identifier (SCI). Each node, which expects to receive traffic sent through a particular transmit secure channel, must configure a matching receive secure channel. This receive secure channel must have an SCI corresponding to the SCI of the transmit secure channel of the peer.

Secure Association:

Within each secure channel (both transmit and receive,) Secure Associations are defined. Each secure association has a corresponding Secure Association Key (the encryption/decryption key) and is identified by the Association Number field of the SecTAG header. Secure associations have limited duration, hence both sides need to establish a new secure association and switch to it before the old one expires, which is called Key Rotation.

Packet Number and Replay Protection:

Within each secure association, replay protection can be performed by checking the Packet Number field of SecTAG header against the packet number locally stored. Each MACsec packet has a unique sequential packet number and each packet number can only be used once in a given secure association.

How MACsec handles data and control traffic:

All traffic is controlled on an active MACsec port where data is encrypted, or its integrity is protected, or both. If a MACsec session cannot be secured, all data and control traffic are dropped.

When MACsec is active on a port, the port blocks the flow of data traffic. Data traffic is not forwarded by the port until a MACsec session is secured. If an ongoing session is torn down, traffic on the port is again blocked until a new secure session is established.

Control traffic (such as STP, LACP or UDLD traffic) is not transmitted by an active MACsec port until a MACsec session is secured. While a session is being established, only 802.1X protocol packets are transmitted from the port. Once a secure session is established, control traffic flows normally through the port.

5.0 Automotive Use Cases

Automotive Use Cases showing how MACsec-enabled Phys can be used to protect Ethernet vulnerabilities within a Vehicle.

Figure 5 shows the Ethernet links that are the most vulnerable to an attack.

Figures 6a to 6f: Demonstrate a typical attack vector on a 100/1000 BASE-T1 link, and how MACsec can be used to thwart it.

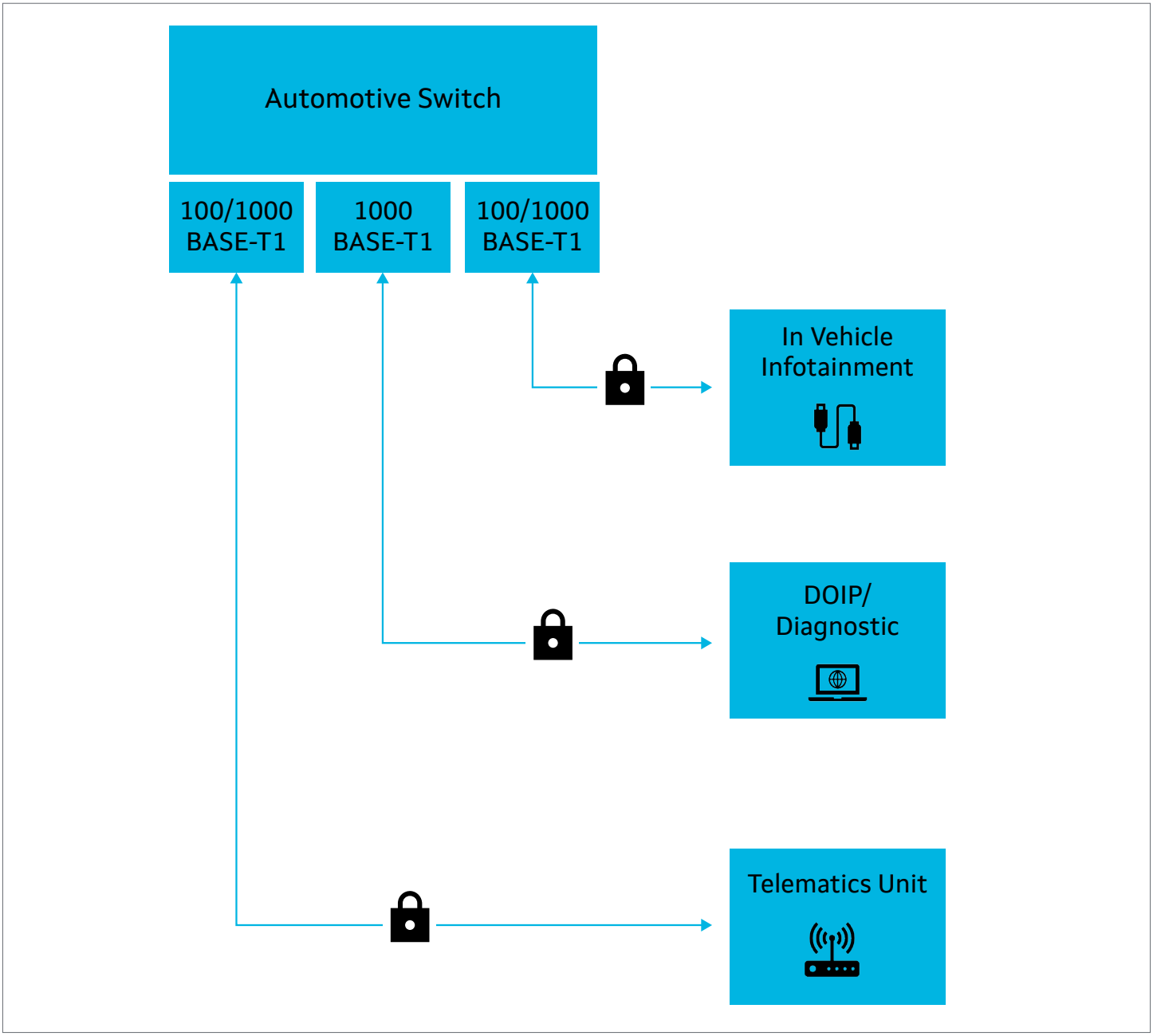

Figure 5: Use Case showing three potential Ethernet links that could be protected by MACsec.

In this use case, a camera is connected via a single 1000 BASE-T1 Ethernet link to a subsystem containing at least a processing unit and a display. The link is facilitated by 2x Marvell 88Q22XXM “Ash” devices that leverage MACsec feature as defined in IEEE Standard 802.1AE. The link could have an inline connector, presenting a hacker with the opportunity to steal data and/or disrupt communication. Figures 6a and 6b demonstrate this potential use case and its inherent vulnerabilities.

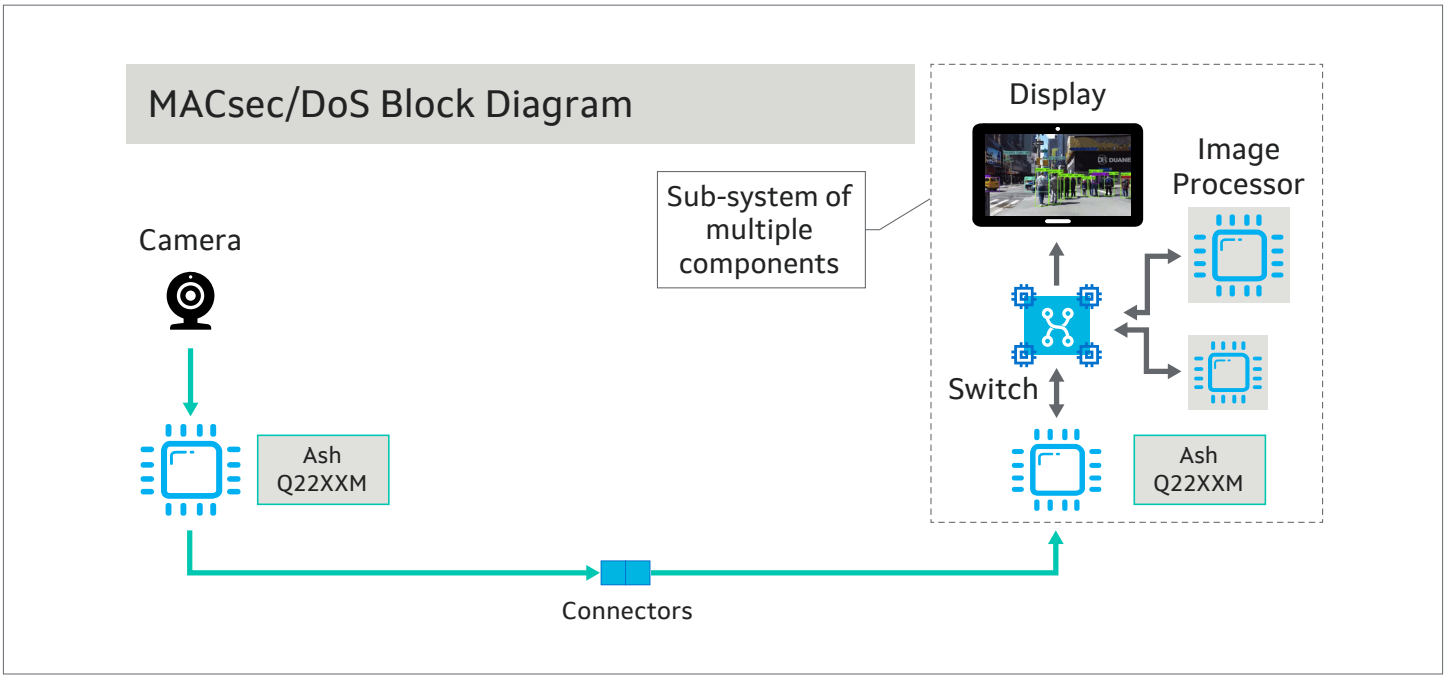

Figure 6a: Camera and Display sub-system communicating via a cable and an Inline Connector.

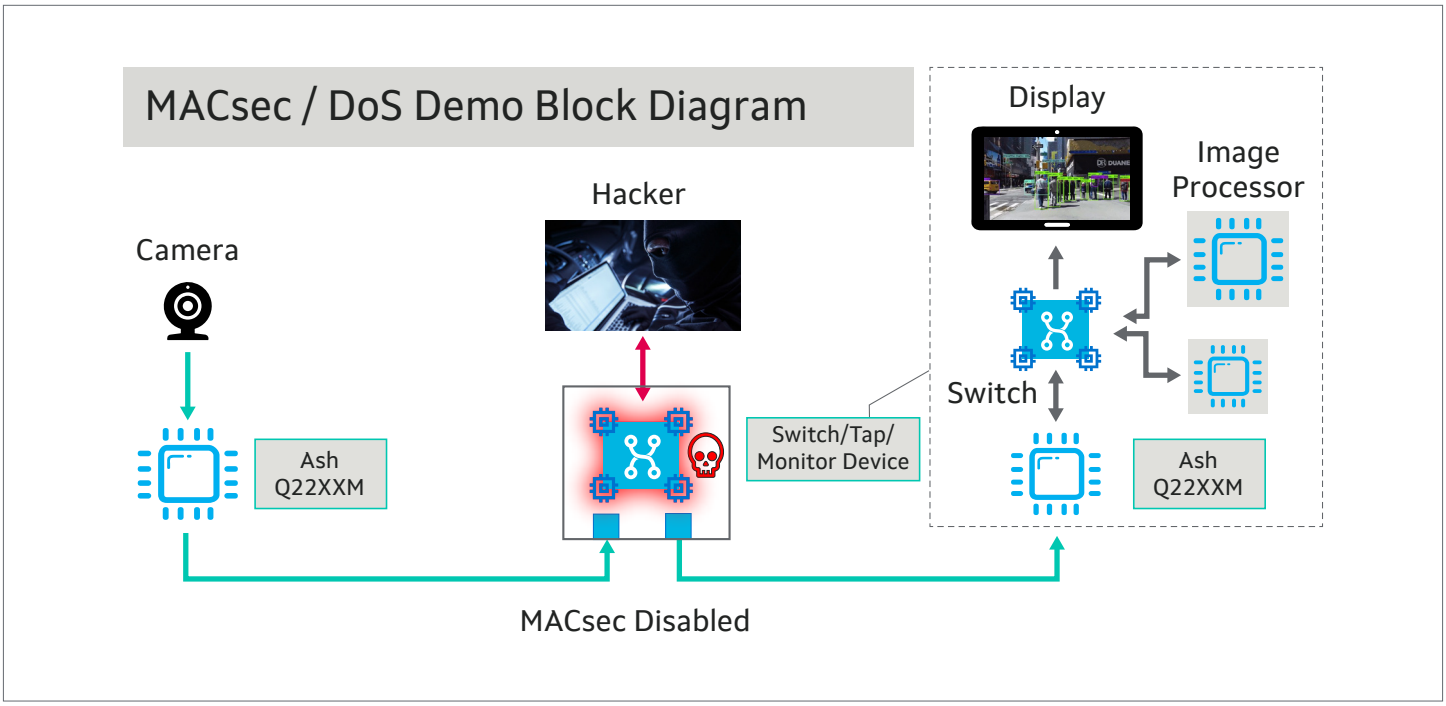

Figure 6b: Hacker is able to tap into the Ethernet Network using their own Switch, or a Repeater/Monitor device.

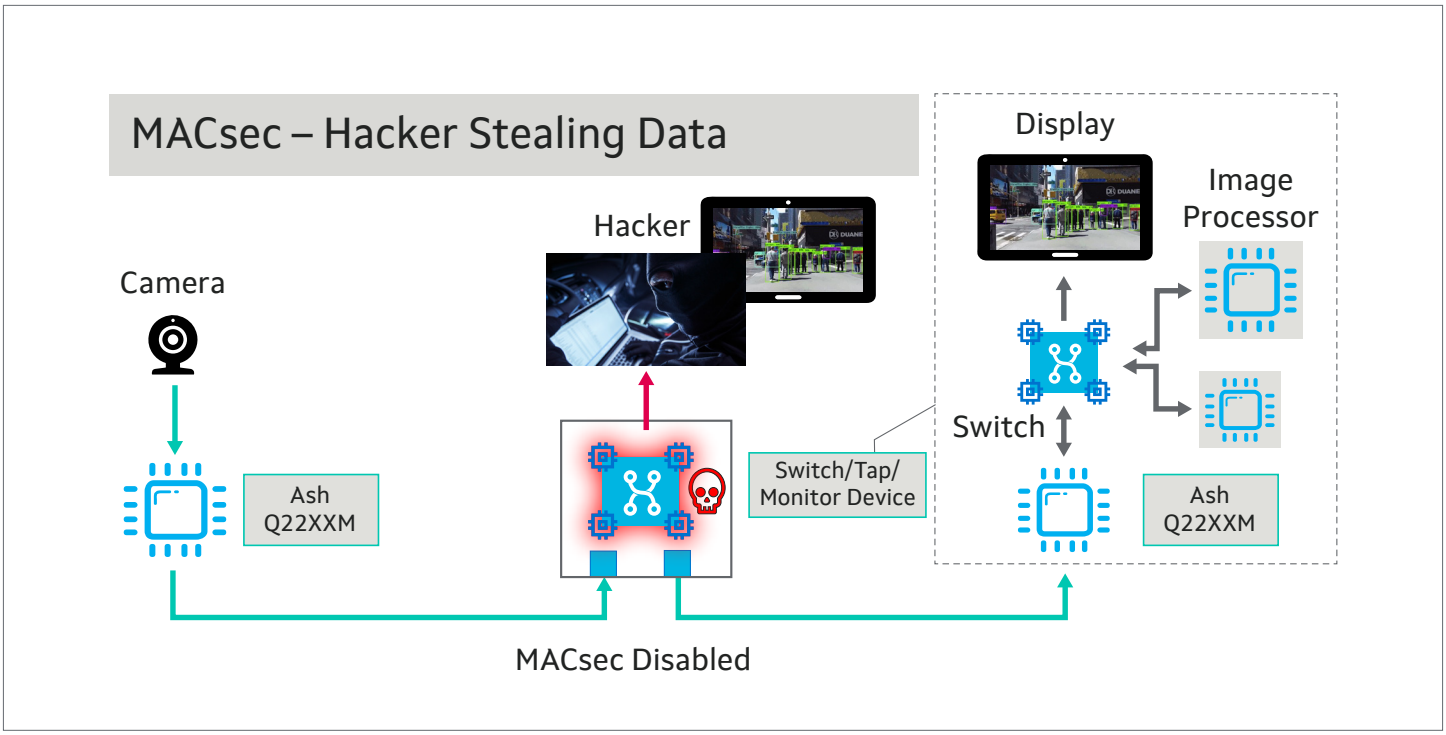

Figure 6c: Hacker can steal the data

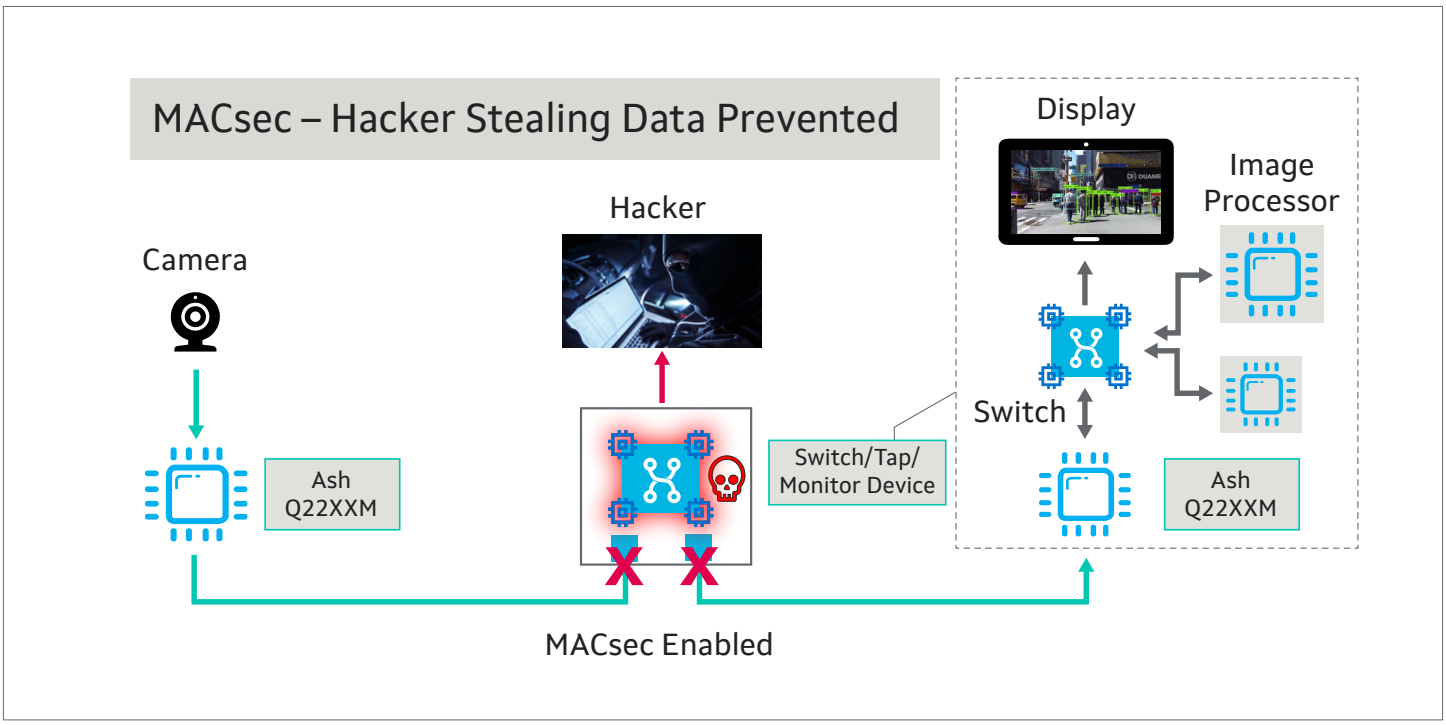

Figure 6d: MACsec encryption between the PHYs prevents the hacker from understanding the data

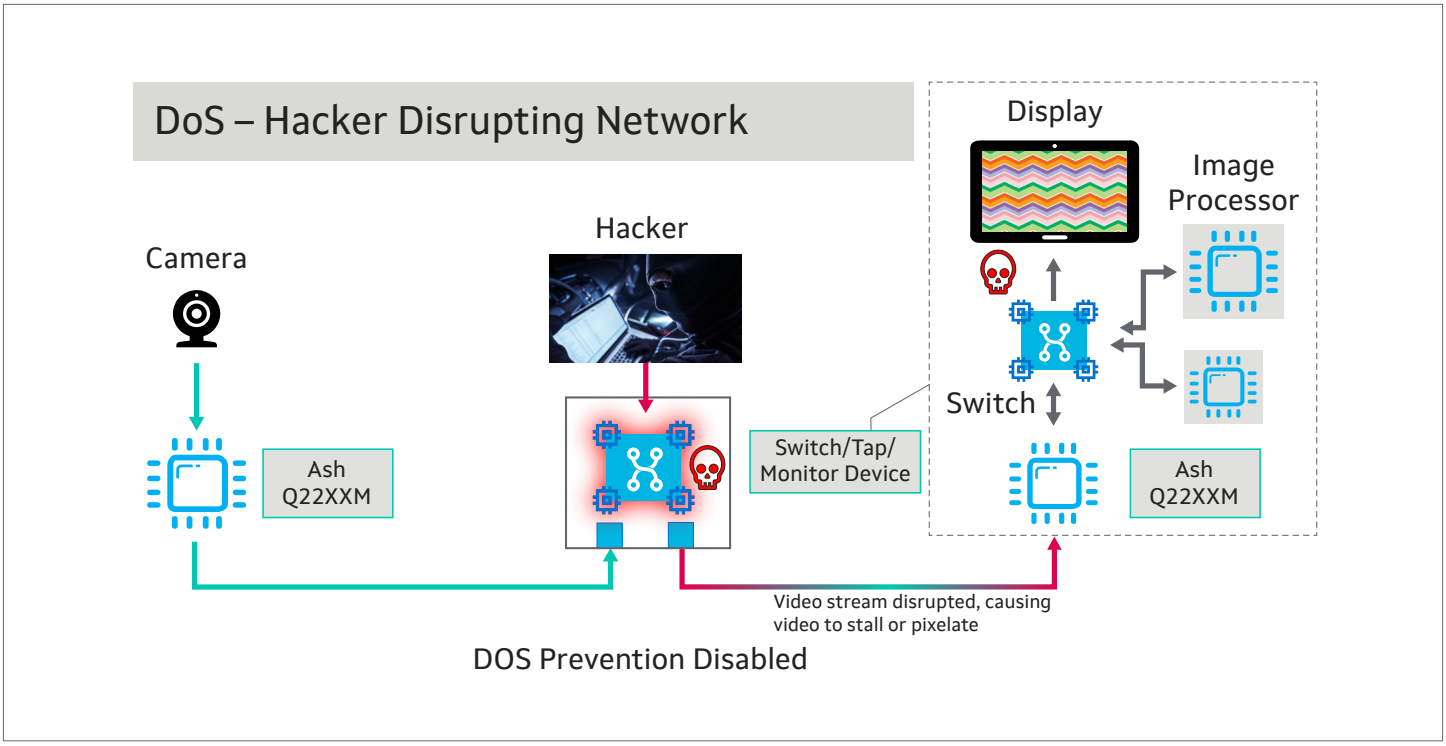

Figure 6e: Hacker executes Denial-Of-Service attack on the Image processing sub-system and jams the link.

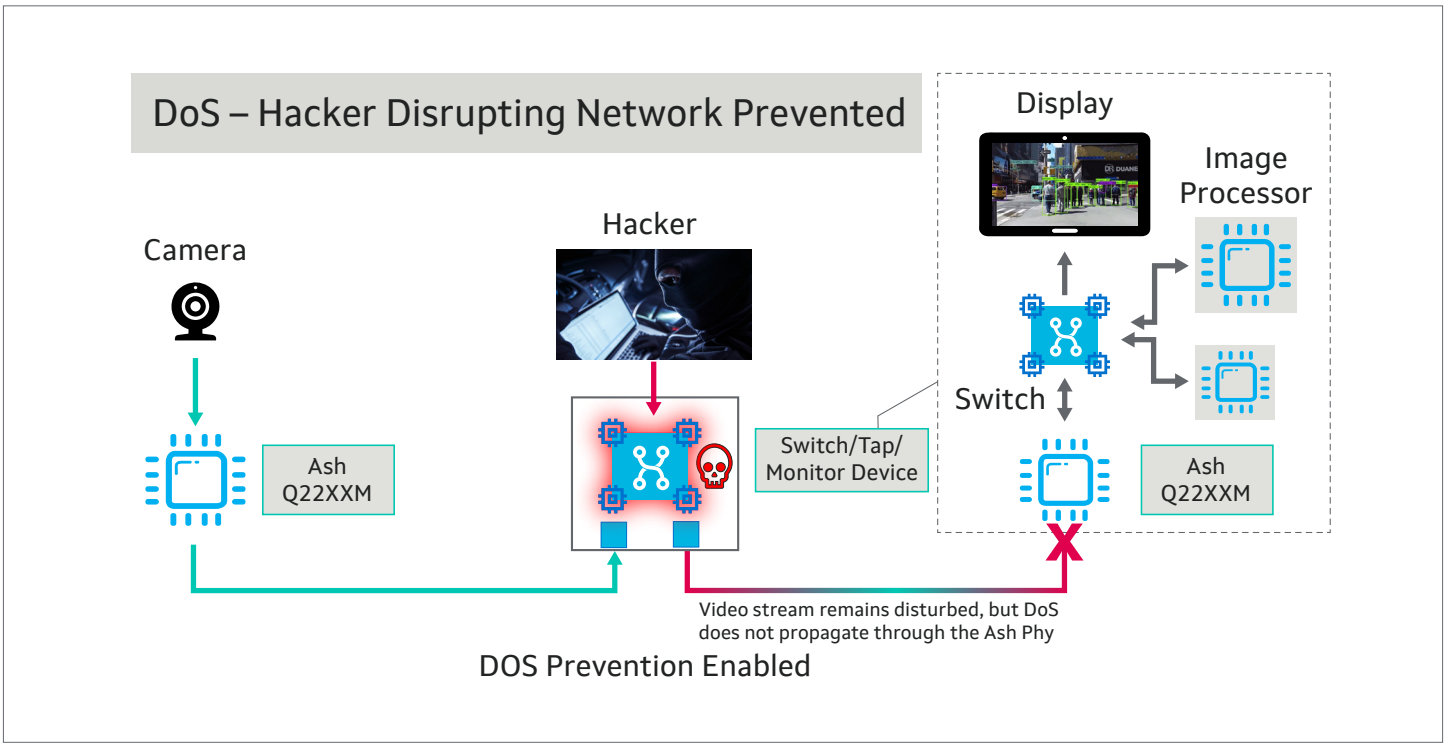

Figure 6f: DoS data from hacker is dropped by Ash PHY connected to Image processing sub-system due to key mismatch.

Additional security measures need to be considered:

- Unused switch/SoC ports are disabled in hardware.
- Various Ingress policy tools prevent malicious data from targeting unused ports in case the hardware de-activation is bypassed.
- Data on active ports is screened based on expected traffic profile, with suspicious data either being dropped, or forwarded to a firewall.
- The Ingress rate of data that meets the expected traffic profile is policed.

5.2. Secure Phy (Using MACsec and Denial of Service Prevention)

Example Use Case highlights how MACsec implemented at Network hardware level plus Denial of Service (DOS) mechanisms can be used to prevent a Hacker stealing Video data or prevent Hacker disturbing Video data.

6.0 Role of IEEE 802.1X

6.1 What is IEEE 802.1X?

IEEE 802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. Devices attempting to connect to a secure network require an authentication mechanism. IEEE 802.1X, an IEEE Standard for Port-Based Network Access Control (PNAC), provides protected authentication for secure network access.

An 802.1X network is different from home networks in one major way: it has an authentication server called a RADIUS Server. It checks a user's credentials to see if they are an active member of the organization and, depending on the network policies, grants users varying levels of access to the network. This allows unique credentials or certificates to be allocated per user, eliminating the reliance on a single network password that can be easily stolen. The RADIUS server is able to do this by communicating with the organization's directory, typically over the LDAP or SAML protocol.

6.2 How does Authentication work per 802.1X?

The authentication process comprises four steps:

- Initialization
- Initiation
- Negotiation
- Authentication

Initialization

The Initialization step starts when the authenticator detects a new device and attempts to establish a connection. The authenticator port is set to an "unauthorized" state, meaning that only 802.1X traffic will be accepted and every other connection will be dropped.

Initiation

The authenticator starts transmitting EAP1 (Extensible Authentication Protocol) requests to the new device, which then sends EAP responses back to the authenticator. The response usually contains a way to identify the new device. The authenticator receives the EAP response and relays it to the authentication server in a Radius2 (Remote Authentication Dial-In User Service) access request packet.

[1]As defined by Wikipedia: Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections. It is defined in RFC 3748, which made RFC 2284 obsolete, and is updated by RFC 5247. EAP is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods. There are many methods defined by RFCs and a number of vendor-specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines the information from the interface and the formats. Each protocol that uses EAP defines a way to encapsulate by the user EAP messages within that protocol's messages.

[2]RADIUS is a client/server protocol that runs in the application layer and can use either TCP or UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication as well (Wikipedia.)

Negotiation

Once the authentication server receives the request packet, it will respond with a RADIUS access challenge packet containing the approved EAP authentication method for the device. The authenticator will then pass on the challenge packet to the device to be authenticated.

6.3 MACsec Key Agreement Protocol

- MACsec Key Agreement (MKA) protocol installed on a device relies on an IEEE 802.1X Extensible Authentication Protocol (EAP) framework to establish communication.
- MACsec peers on the same LAN belong to a unique connectivity association. Members of the same connectivity association identify themselves with a shared Connectivity Association Key (CAK) and Connectivity Association Key Name (CKN). The CAK is a static key that is preconfigured on each MACsec-enabled interface. MACsec authentication is based on mutual possession and acknowledgment of the preconfigured CAK and Connectivity Association Key Name (CKN).
- Each peer device establishes a single unidirectional secure channel for transmitting MACsec frames (Ethernet frames with MACsec headers that usually carry encrypted data) to its peers within the connectivity association. A connectivity association consists of two secure channels, one for inbound traffic, and one for outbound traffic. All peers within the connectivity association use the same cipher suite, either Galois/Counter Mode Advanced Encryption Standard 128 or 256 (GCM-AES-128 or GCM-AES-256), for MACsec-authenticated security functions.
- MACsec Key Agreement (MKA) protocol uses the Connectivity Association Key to derive transient session keys called Secure Association Keys (SAKs). SAKs and other MKA parameters are required to sustain communication over the secure channel and to perform encryption and other MACsec security functions. SAKs, along with other essential control information, are distributed in MKA protocol control packets, also referred to as MKPDUs.

6.4 MKA message exchange between two switches

- When two MACsec peers confirm possession of a shared CAK and CKN, MKA protocol initiates key-server election.
- The key-server is responsible for determining whether MACsec encryption is used and what cipher suite is used to encrypt data. The key-server is also responsible for generating SAKs and distributing them to the connected device. Once a SAK is successfully installed, the two devices can exchange secure data.
- The following figure shows the message flow between two switches during MACsec communication.

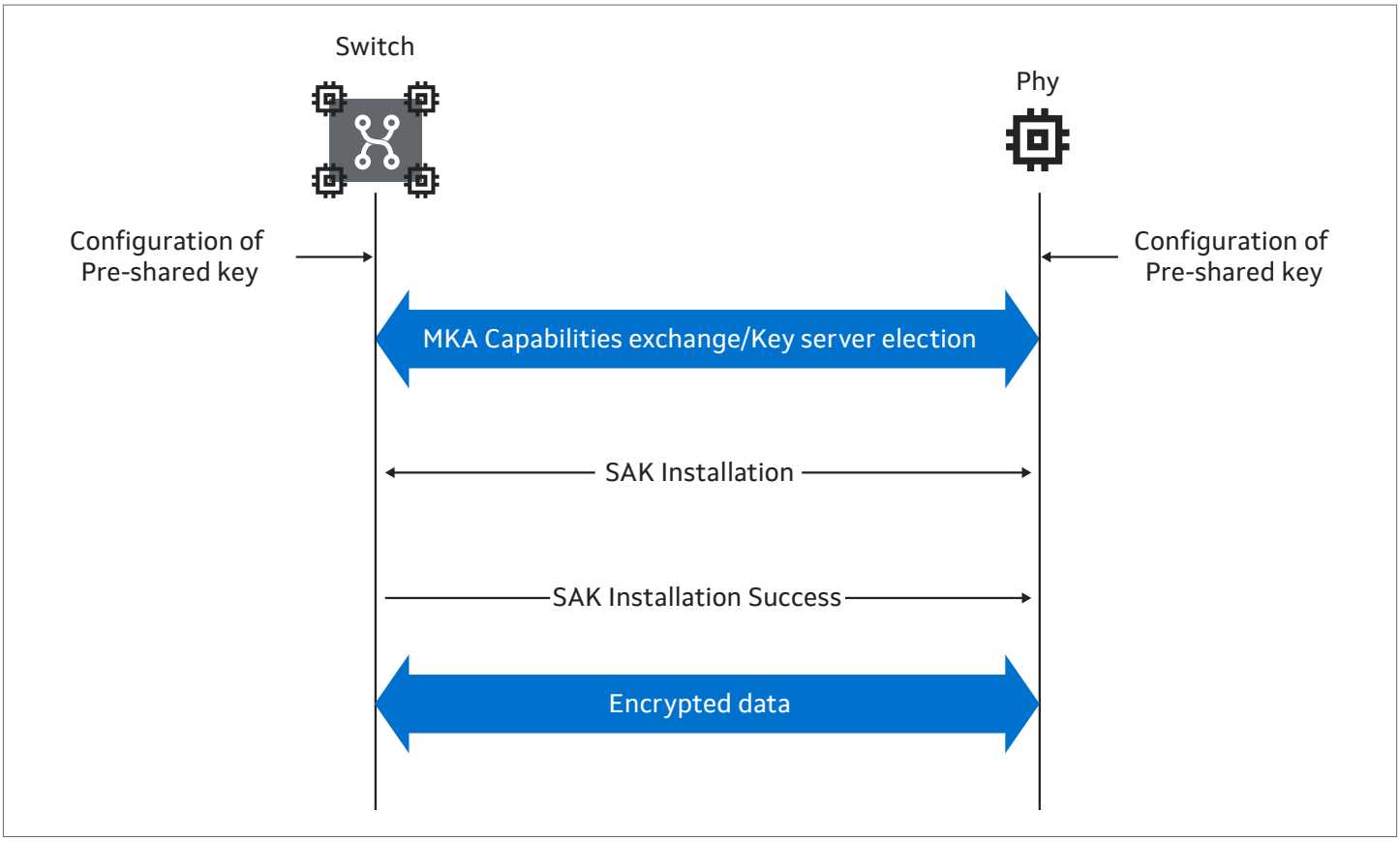

Figure 7: MACsec Message Exchange Mechanism

7.0 MACsec main features and its advantages for Automotive

Using MACsec which has built in encryption/decryption and if we combine this with Key agreement (Authentication), we could be use within the Automotive sector. Vehicle manufacturers could enforce MACsec protection on the most vulnerable Ethernet links which are exposed to the outside world. As always with security-related matters, careful considerations are needed to eliminate security vulnerabilities. MACsec a cost-effective security tool, within the overall armoury of Automotive Security toolbox that systems Engineers could use in combination with other security tools like IPSec and TLS.