

Ethernet Security- how effective is it?

Rajeev Roy, NXP
Balaji Arumugam, Garrett

IEEE Ethernet & IP Tech Days – September 2023



SECURE CONNECTIONS
FOR A SMARTER WORLD

Garrett

ADVANCING MOTION

PUBLIC



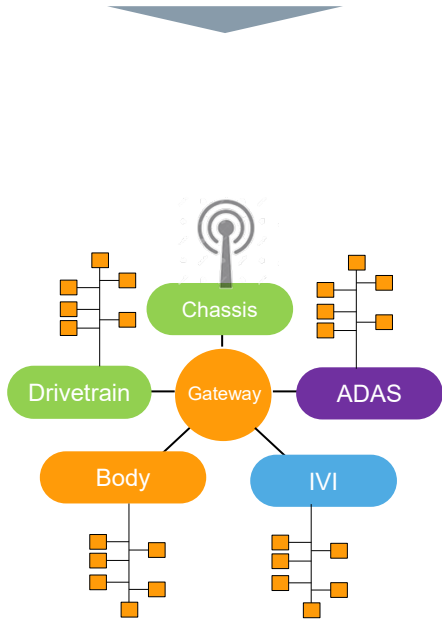


OVERVIEW

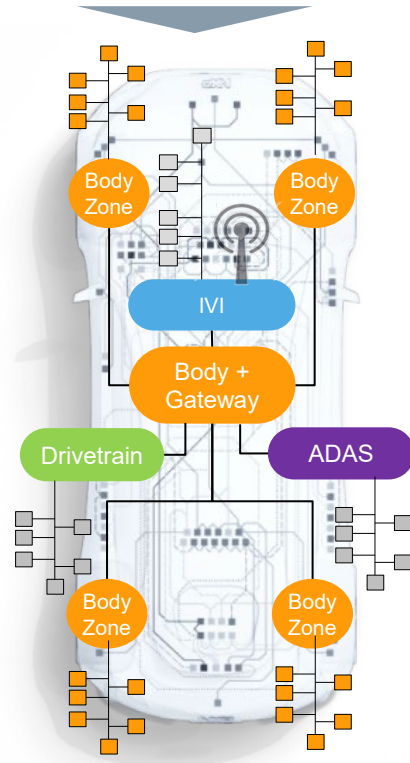
- Evolving network architecture and security challenges
- Holistic view- setting the context
- The Ethernet Angle
 - Secure Interfaces
 - Secure Domain
 - Secure Networks
 - Secure Infrastructure (processing)

VEHICLE ARCHITECTURE EVOLVING ACROSS DOMAIN AND ZONE AXIS

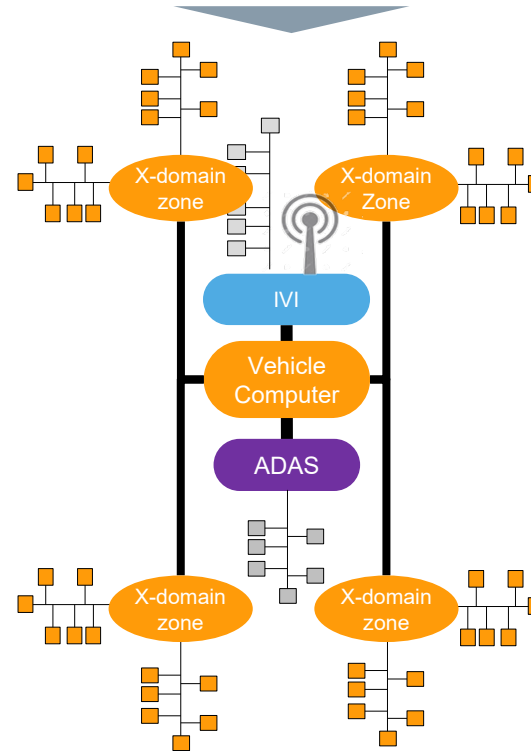
DOMAIN BASED VEA



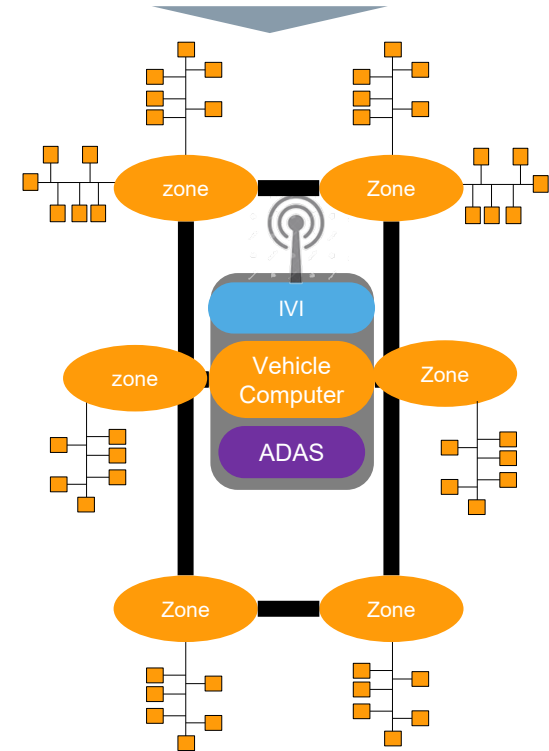
BODY ZONAL VEA



CROSS-DOMAIN ZONAL VEA



SDV-OPTIMIZED VEA

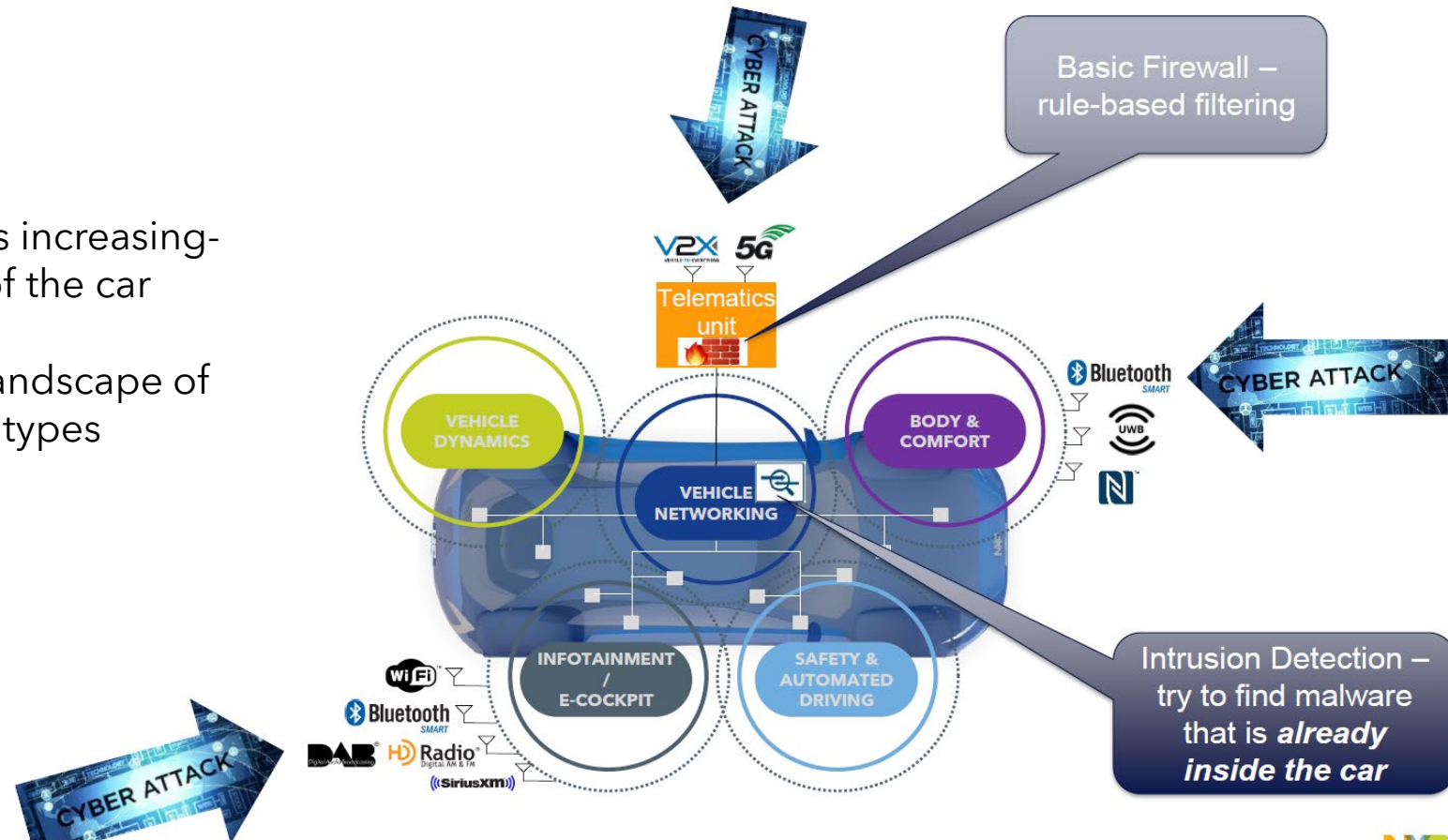


WHY ARE THE SECURITY CHALLENGES INCREASING FOR SDV?






SECURITY- WHY ARE THE CHALLENGES INCREASING?

Surface area for attacks is increasing-
both in-car and out of the car

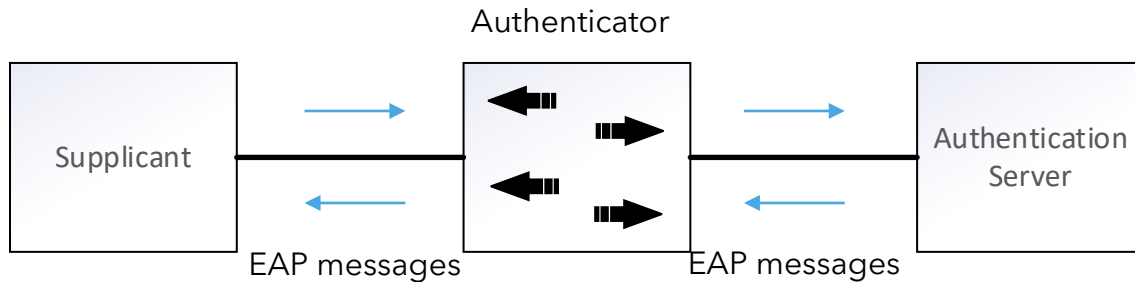
Continuously evolving landscape of
attacks and attack types



HOLISTIC APPROACH- SETTING THE CONTEXT

		PREVENT ACCESS	DETECT ATTACKS	REDUCE IMPACT	FIX VULNERABILITIES
SECURE INTERFACES		M2M Authentication & Firewalling	Secure Ranging (UWB)		
SECURE DOMAIN ISOLATION		Firewalling, VLAN, ...	Network Intrusion Detection Systems (NIDS)	Separated Functional Domains	Secure Updates
SECURE NETWORKS		Secure Messaging		Message Filtering & Rate Limitation	
SECURE PROCESSING		Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	
SECURE ENGINEERING		SDLC incl. Security Reviews & Testing, ...	Threat Monitoring, Intelligence Sharing, ...	Incident Management / Response	
		Security-Aware Organization, Policies, Governance			

SECURE INTERFACES- THE ETHERNET ANGLE



In wired Ethernet, the Extensible Authentication Protocol over LAN (EAPOL) is used for a supplicant to authenticate with an authentication server

EAP: Extended Authentication Protocol

Secure Interfaces: Authentication

IEEE802.1X, Port Based Network Access Control (PNAC) is a common way to authenticate supplicants- it is an industry standard way of authentication and can prevent Man-in-the-Middle (MitM) and Evil Twin proxies

What are the expected requirements?

An authenticator has to block all communication from an unauthorised supplicant (till authenticated) while allowing for EAP messages

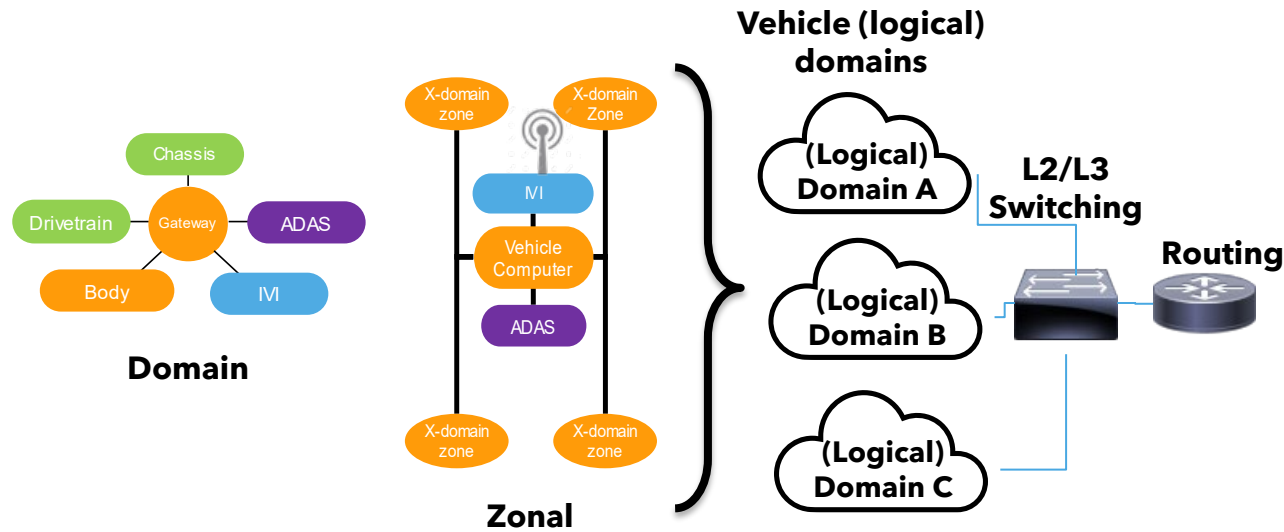
What are the potential threats?

- EAP messages use the multicast address (01:80:c2:00:00:03) and this opens a window of opportunity for flooding (DoS) type attacks;
- MAC migration can lead to frame flooding (and related loss of performance)

How effective is it?

- Is it possible to identify specific (multicast) streams, meter and police them?
- Can stream forwarding be realized?
- Can MAC move be detected and prevented?
- Can MAC limiting be supported?

SECURE DOMAIN ISOLATION- THE ETHERNET ANGLE



Conceptually both domain and zonal network are switched Ethernet networks with the "Gateway" implementing routing functionality; Both architectures would also support tagged networks - but this is a must have for the zonal network

Secure Domain Isolation: VLANs (& IP subnets)

VLANs complement and enhance isolation of a network along with IP subnetting. Partitioning can prevent or mitigate L2 attacks which influence L3 operations like- ARP spoofing (isolating an external entity from gratuitous ARP response), DHCP starvation (port binding and bounding to specific domains)

What are the expected requirements?

VLAN usage in automotive for most OEMs tends to be for functional domain separation with one or more VLANs per logical domains- VIDs also tend to be used as "stream identifiers" for stream based forwarding and/or for diagnostic stream identification

What are the potential threats?

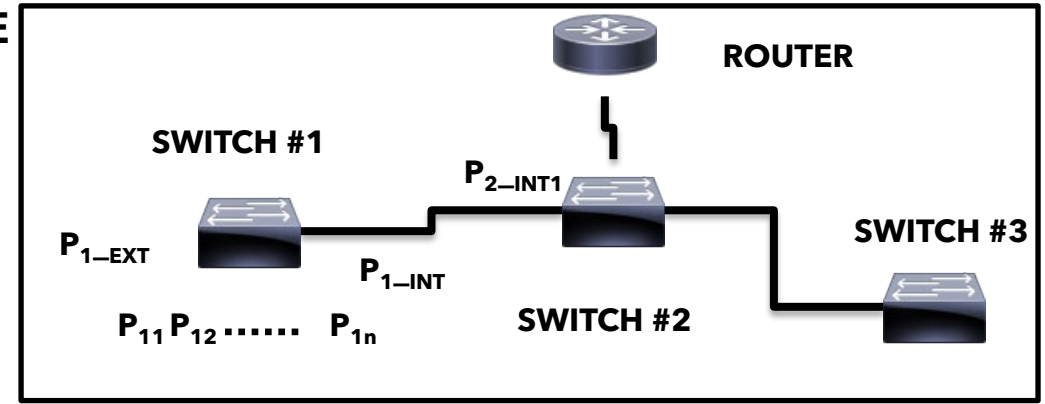
- Leakage of traffic across domains- consequent security and QoS concerns

How effective is it?

- Is the switch core supporting the necessary features?
- How robust is switch core performance for the desired configuration?
- Is there synergy in the L2 and L3 network design for partitioning?
- Is there ability to selectively mirror traffic for diagnostics/monitoring?

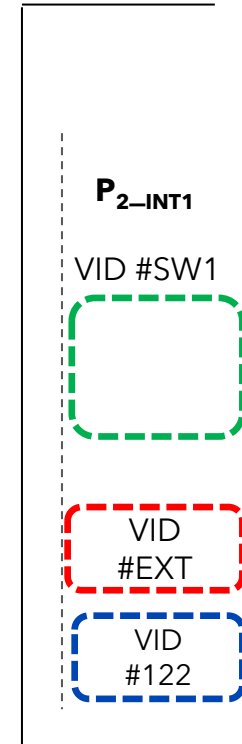
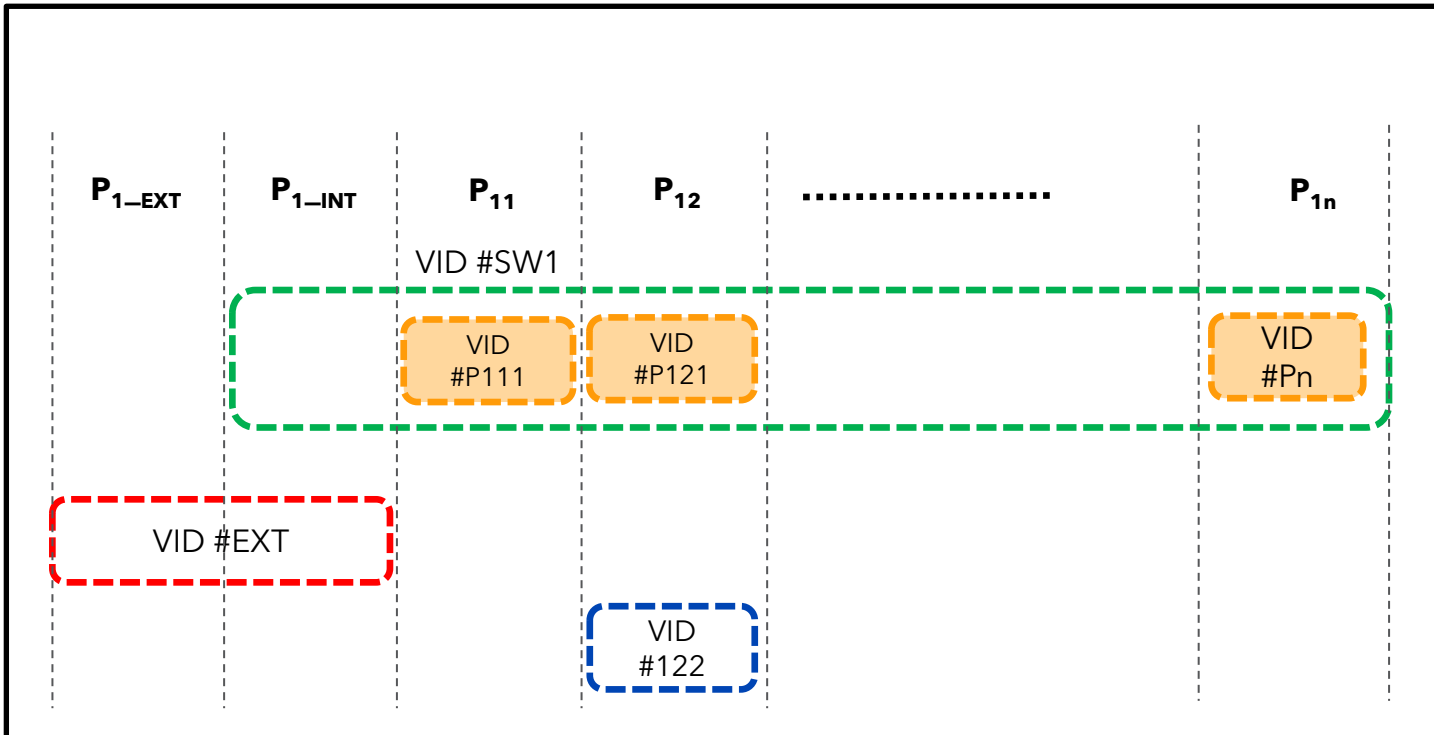
SECURE DOMAIN ISOLATION- THE ETHERNET ANGLE

A typical example of VLANs in Switch #1 and #2 (partly) illustrating how VLANs could be used for isolation- including examples of a primary VLAN with private VLANs, VLAN across two switches and a dedicated VLAN for external traffic;



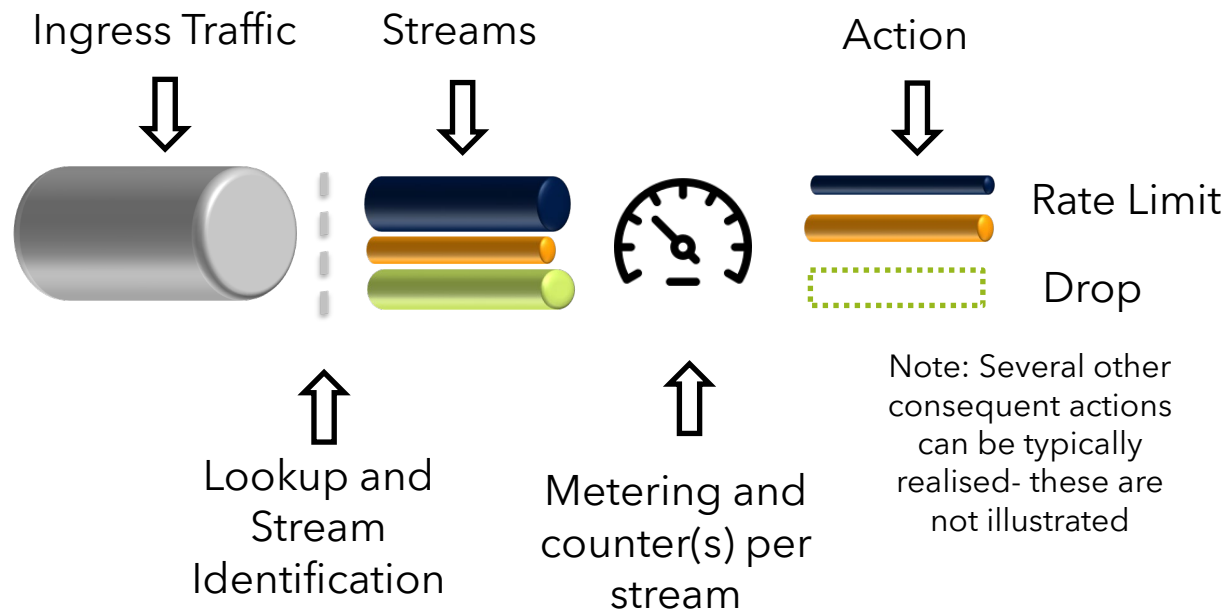
SWITCH #1

SWITCH #2



VLANs not only complement IP subnetting for network partitioning- they are essential to realise isolation

SECURE NETWORKS- THE ETHERNET ANGLE



Secure Networks: Stream Identification, Metering and Filtering

IEEE802.1Qci, Per Stream Filtering and Policing (PSFP) provides a frame work for handling streams, metering and take a consequent action- typical implementations provide more functionality to this by supporting mechanisms for selective mirroring, actions on frames such as- dropping or forwarding/duplicating to designated ports

What are the expected requirements?

Stream (or flow) identification is needed to decide on a consequent action on that stream- typically for implementing rules, policies and for Intrusion Detection and Prevention (ID/PS) systems

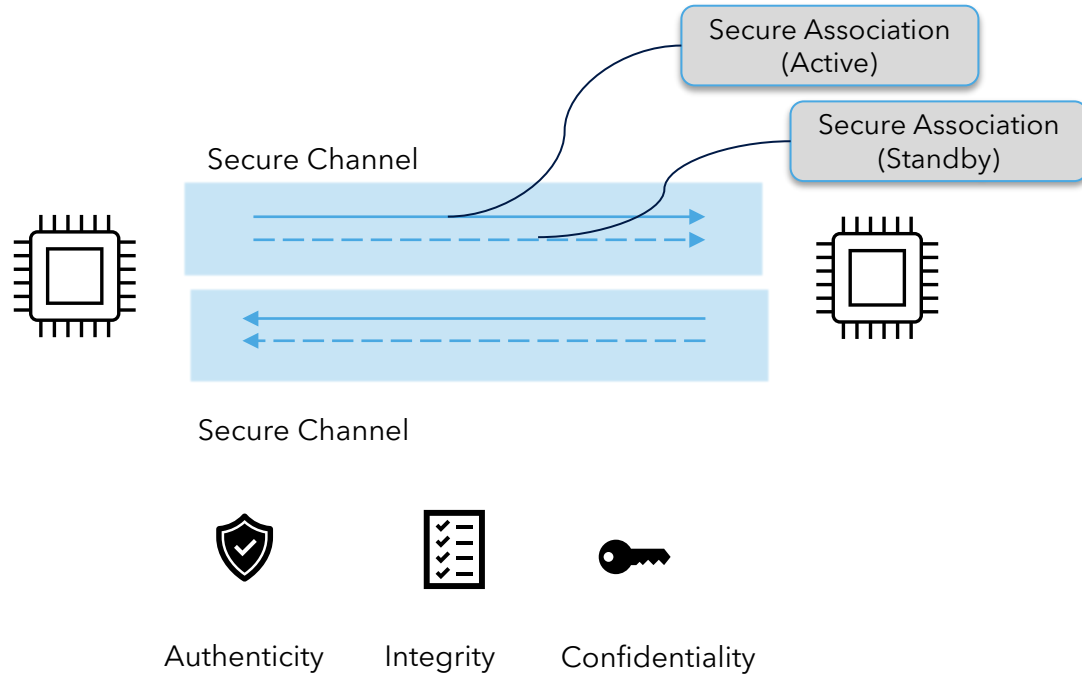
What are the potential threats?

- Potentially stream based decisions can over-ride usual bridging behaviour and can lead to unintended actions on the frame forwarding

How effective is it?

- To what granularity can streams be defined (e.g. filter UDP port from a specific source IP)?
- Can sufficient rules be defined to realise an effective ID/PS implementation?
- Can the streams be properly metered and consequent actions taken?
- Can a proper reconciliation of frame counters be done?

SECURE NETWORKS- THE ETHERNET ANGLE



Secure Networks: MACsec

IEEE802.1AE, MAC Security (MACsec) can ensure authenticity, integrity and confidentiality of data- this is one of the key features seen as a must have to ensure that nodes which can be easily tampered with (e.g. radars on bumpers) can be authenticated. Integrity check ensures against data tampering and encryption ensures confidentiality

What are the expected requirements?

MACsec provides a fast means for authentication - with the benefits of integrity check and encryption

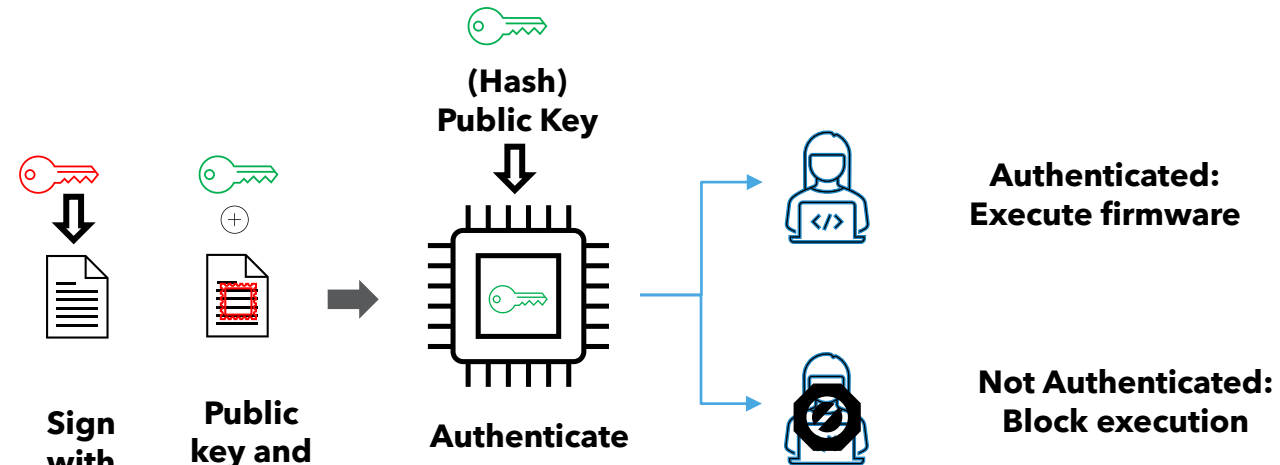
What are the potential threats?

- Compromising the secret keys

How effective is it?

- In automotive applications it is common to use pre-shared keys (PSKs) - is the implementation such that it cannot scale to fleet attacks?
- Standards are in definition for multi drop systems
- Exchange of keys in clear text (e.g. PHYs)?
- Sufficient hardware support for intended CAK?
- XPN supported?

SECURE INFRASTRUCTURE- THE ETHERNET ANGLE



Conceptual view of secure boot with asymmetric encryption- details on Chain of Trust (CoT) etc are not illustrated;

Prevent Access: Secure Boot

Secure boot is a means to boot with authenticated software (firmware) and the process also ensures the integrity of the software.

What are the expected requirements?

Device can boot using authenticated software in the specified start up time

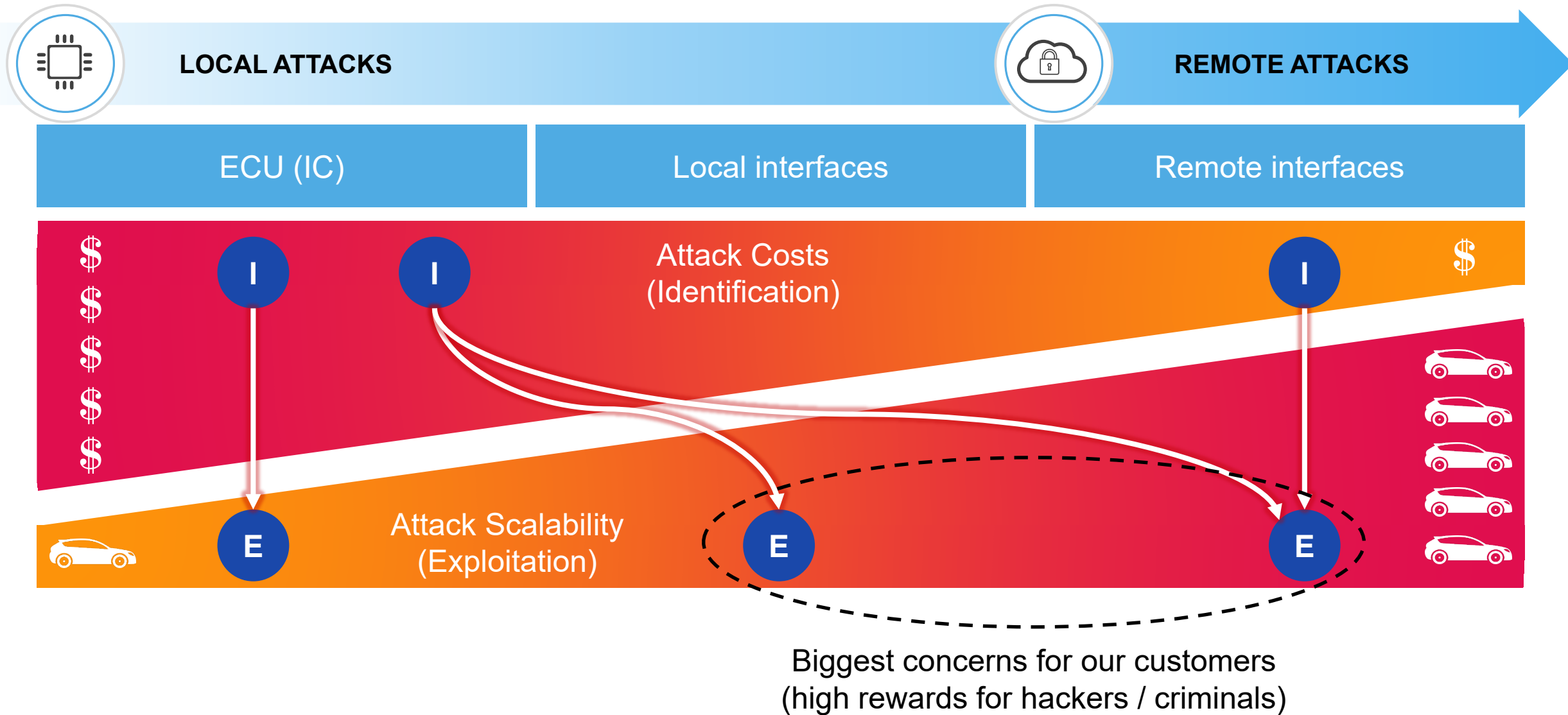
What are the potential threats?

- Implementation which stores secrets for authentication without sufficient safe-guards

How effective is it?

- What is the security strength of the encryption technology?
- Are any secrets stored in the device- and if so, is the device hardened?
- Are there sufficient hardware accelerators to ensure a start up time as per specifications?
- Is a chain of trust built in?
- Is there a version numbering built in?
- Is there a bypass for secure-boot?

ATTACK COSTS VS. ATTACK SCALABILITY



I Identify vulnerability **E** Exploit vulnerability

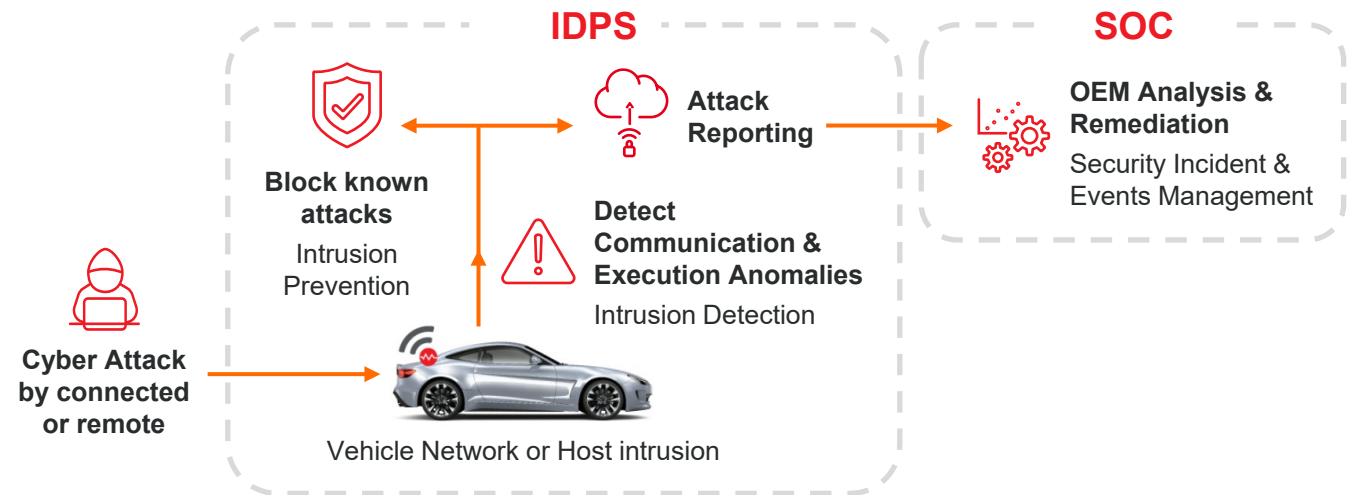
Enhancing security with Network IDPS

What is NIDPS?

- **N**etwork **I**ntrusion **D**etection and **P**rotection **S**ystem
- Modeling of known behaviors on network and alert on violations
- Software or/and Hardware Solution

What are the key features?

- Vehicle context-based evaluation
- Hardware accelerated detectors
- Stateful analysis/inspection
- Deep Packet Inspection - from L2 to L5 (application layer)
- Rule-based evaluation with Signatures and Patterns or ML/AI approach
- Anomaly reports with meaningful information



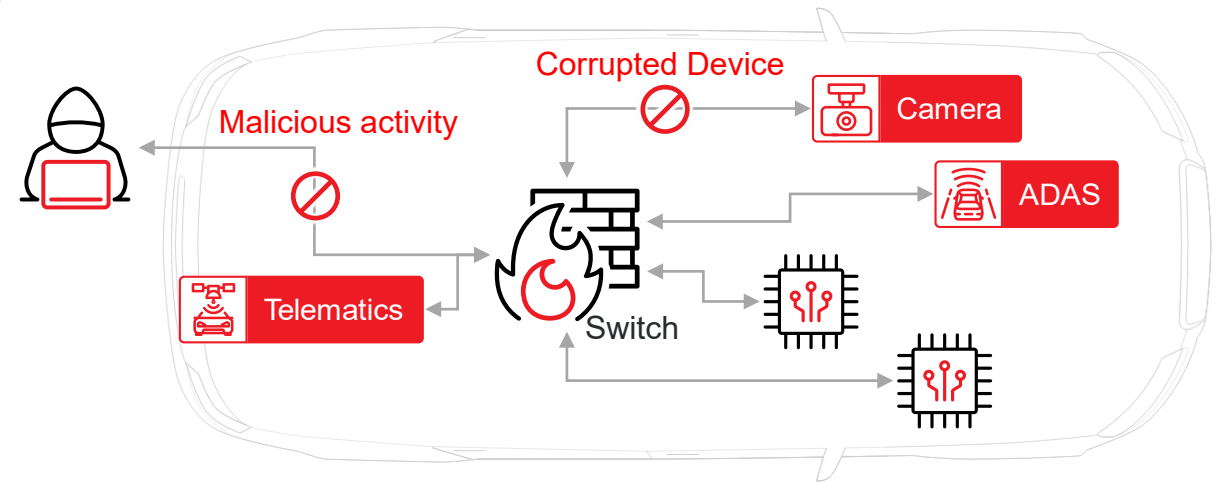
Network IDPS

What it does?

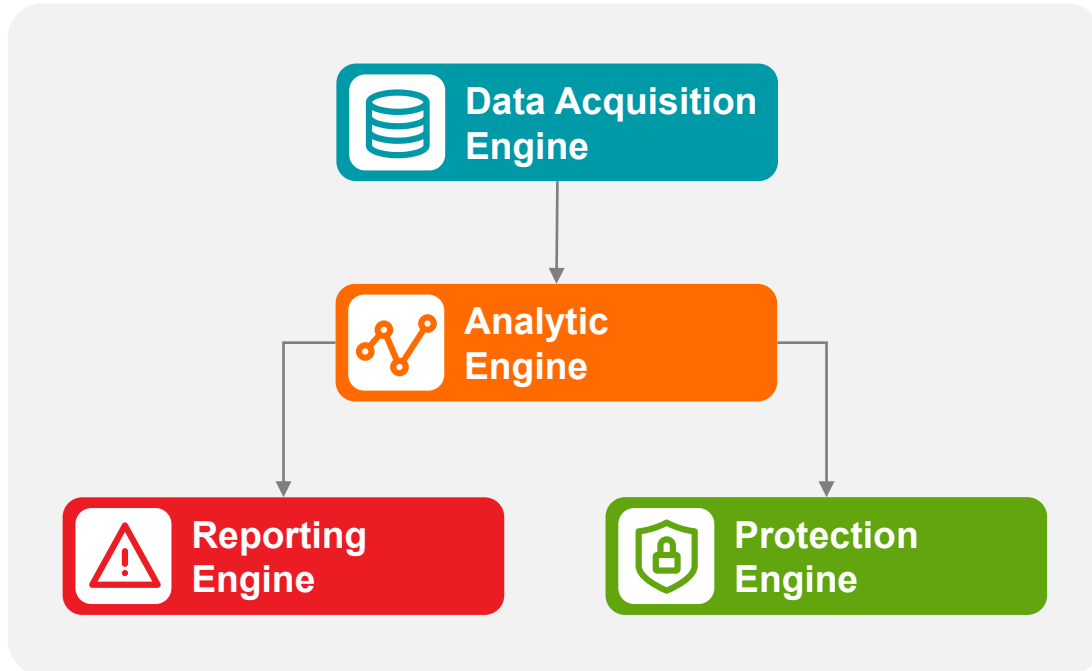
- Monitors network traffic in order to detect:
 - Unknown/Abnormal/Invalid traffic(e.g.: New Connection)
 - Attacks (e.g.: D/Dos, Man in the Middle)
 - Harmful patterns (e.g.: Teardrop)
- Reports anomalies
- Prevents detected threats


Why is switch (Firewall) not enough?

- Cannot inspect payload for threat patterns
- Cannot detect if a device from the network is corrupted
- Cannot monitor and prevent malicious activity for both internal and external communication
- Cannot report malicious activity (e.g.: new device is connected to the network or corrupted network devices)



Network IDPS Architecture



 **Data Acquisition Engine**

Captures traffic from specific protocol layer

- RAW, IP, Socket etc.

 **Analytic Engine**

Analyze incoming traffic based on

- Signatures
- Patterns
- Heuristic
- ML / AI

 **Protection Engine**

Block attacks by

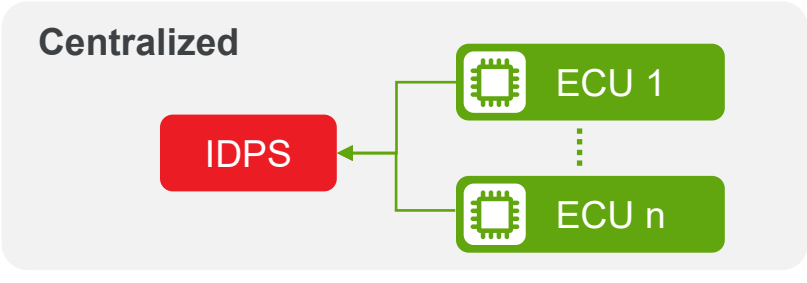
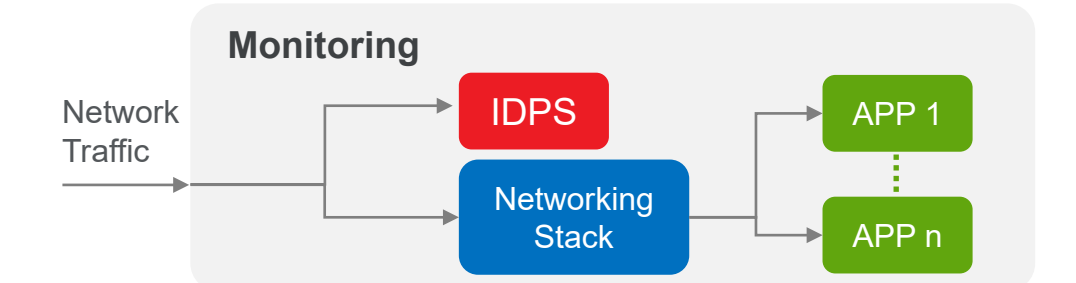
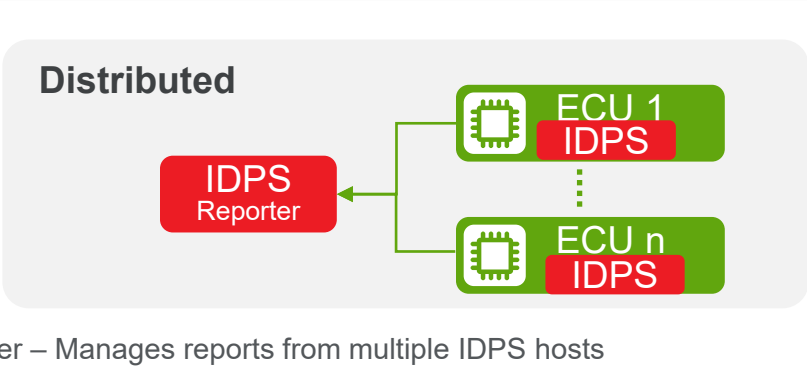
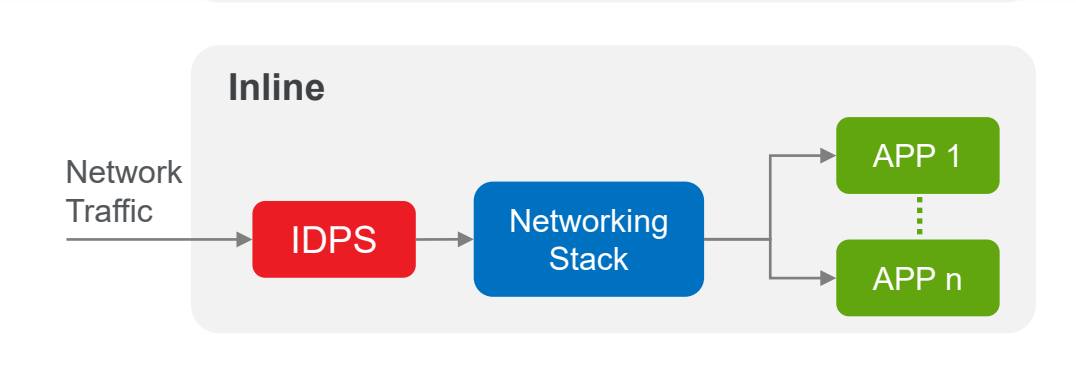
- Dropping packets
- Configuring Switch
- Configuring OS firewall

 **Reporting Engine**

Report detected anomalies to

- System Log
- IDS Reporter
- Cloud (V-SOC)

Network IDPS Deployment Types & Configurations

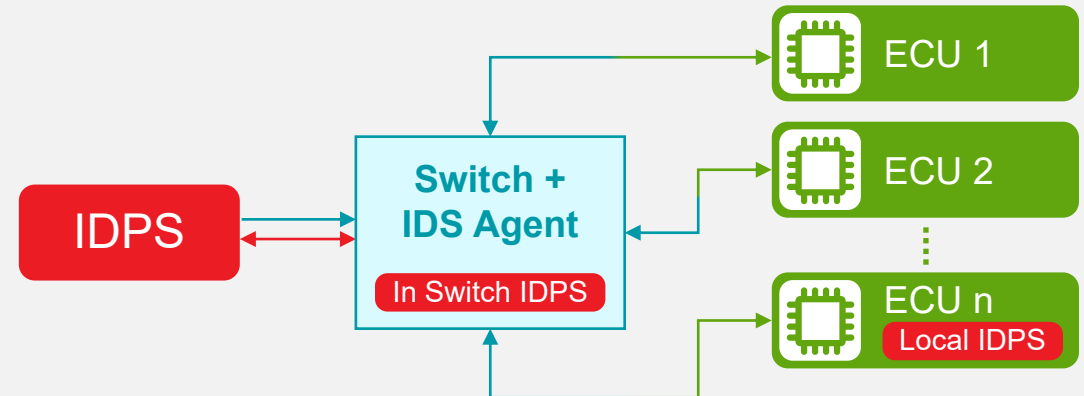
DEPLOYMENT TYPES	CONFIGURATIONS
<ul style="list-style-type: none">• Centralized – IDPS hosted on one processor• Distributed – IDPS hosted on multiples processors	<ul style="list-style-type: none">• Monitoring – Analyzing the traffic passively• Inline – Analyzing the traffic actively
<p>Centralized</p>  <p>The diagram shows a central red box labeled 'IDPS' on the left. Two green boxes representing ECUs, 'ECU 1' and 'ECU n', are on the right. Green arrows point from each ECU box to the central IDPS box, indicating that traffic from both ECUs is sent to a single central IDPS processor.</p>	<p>Monitoring</p>  <p>The diagram shows 'Network Traffic' entering from the left. The traffic splits into two paths: one goes to a red box labeled 'IDPS' and the other goes to a blue box labeled 'Networking Stack'. Both paths then merge and lead to two green boxes representing applications, 'APP 1' and 'APP n', on the right. This represents a passive monitoring configuration where traffic is analyzed before reaching the applications.</p>
<p>Distributed</p>  <p>The diagram shows a red box labeled 'IDPS Reporter' on the left. Two green boxes representing ECUs, 'ECU 1' and 'ECU n', are on the right. Each ECU box contains a smaller red box labeled 'IDPS'. Green arrows point from each of these local IDPS boxes to the central 'IDPS Reporter' box, indicating that each ECU has its own IDPS and reports back to a central manager.</p> <ul style="list-style-type: none">• Reporter – Manages reports from multiple IDPS hosts	<p>Inline</p>  <p>The diagram shows 'Network Traffic' entering from the left and passing through a red box labeled 'IDPS'. The traffic then passes through a blue box labeled 'Networking Stack' before reaching two green boxes representing applications, 'APP 1' and 'APP n', on the right. This represents an active inline configuration where traffic is analyzed and potentially blocked or modified before reaching the applications.</p>

Either deployment type can support any configuration

Network IDPS and Switch Integration

- Integration with Ethernet Switch provides capability to optimize performance
- Enhance overall capabilities to implement anomaly-based protection
- Support both types of deployments – Central and Distributed

Example architecture with switch



IDS Agent – Module performing protection actions

Network IDPS perfect solution ?



Dependent on hardware capability and prioritization

- Needs to be updated constantly to cover new attacks
- Overall IDPS solution requires real world data and feedback loop
- High false positive rates if IDPS model not developed with stable design
- Not able to detect harmful patterns if traffic is encrypted



Summary

- From a holistic view- Ethernet (traffic) related mechanisms can only address a small part of the picture
 - These focus on traffic aspects of authentication, encryption, traffic identification and traffic management
 - The techniques themselves are effective for the scope of operation
- Several factors determine how effective they are and it is important to address these
 - “Defence in depth” is a mantra which is very relevant for security- so while we address only a small part of the picture- care needs to be taken in the implementation to make them effective
 - All the aspects discussed can be prevented from scaling up to fleet attacks- when properly implemented
- IDPS forms an essential element of security, a firewall in isolation is not enough and the IDPS needs sufficient amount of hardware hooks to provide an effective cover





SECURE CONNECTIONS
FOR A SMARTER WORLD

Garrett
ADVANCING MOTION