Ethernet Security - how effective is it?

Rajeev Roy, NXP
Balaji Arumugam, Garrett

IEEE Ethernet & IP Tech Days – September 2023
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

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

<table>
<thead>
<tr>
<th>Secure Interfaces</th>
<th>Prevent Access</th>
<th>Detect Attacks</th>
<th>Reduce Impact</th>
<th>Fix Vulnerabilities</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Secure Domain Isolation</th>
<th>Prevent Access</th>
<th>Detect Attacks</th>
<th>Reduce Impact</th>
<th>Fix Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalling, VLAN, ...</td>
<td>M2M Authentication &amp; Firewalling</td>
<td>Secure Ranging (UWB)</td>
<td>Separated Functional Domains</td>
<td>Secure Updates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Networks</th>
<th>Prevent Access</th>
<th>Detect Attacks</th>
<th>Reduce Impact</th>
<th>Fix Vulnerabilities</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Secure Processing</th>
<th>Prevent Access</th>
<th>Detect Attacks</th>
<th>Reduce Impact</th>
<th>Fix Vulnerabilities</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Secure Engineering</th>
<th>Prevent Access</th>
<th>Detect Attacks</th>
<th>Reduce Impact</th>
<th>Fix Vulnerabilities</th>
</tr>
</thead>
</table>

- **Secure Messaging**
- **Secure Ranging (UWB)**
- **Network Intrusion Detection Systems (NIDS)**
- **Message Filtering & Rate Limitation**
- **Resource Control (virtualization)**
- **Separation Functional Domains**
- **Secure Updates**
- **Security-Aware Organization, Policies, Governance**
- **Threat Monitoring, Intelligence Sharing, ...**
- **SDLC incl. Security Reviews & Testing, ...**
- **Threat Monitoring, Intelligence Sharing, ...**
- **Incident Management / Response**
Secure Interfaces: Authentication

IEEE 802.1X, 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: 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?
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;

VLANs not only complement IP subnetting for network partitioning- they are essential to realise isolation.
Secure Networks: Stream Identification, Metering and Filtering

IEEE802.1Qci, Per Stream Filtering and Policing (PSFP) provides a framework 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?


**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 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.
Secure Infrastructure - The Ethernet Angle

**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

LOCAL ATTACKS

ECU (IC)  |  Local interfaces

REMOTE ATTACKS

Attack Costs (Identification)

Attack Scalability (Exploitation)

Biggest concerns for our customers (high rewards for hackers / criminals)

I  Identify vulnerability  E  Exploit vulnerability
Enhancing security with Network IDPS

What is NIDPS?

- **Network Intrusion Detection and Protection System**
- 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

<table>
<thead>
<tr>
<th>DEPLOYMENT TYPES</th>
<th>CONFIGURATIONS</th>
</tr>
</thead>
</table>
| • Centralized – IDPS hosted on one processor  
• Distributed – IDPS hosted on multiples processors | • Monitoring – Analyzing the traffic passively  
• Inline – Analyzing the traffic actively |

### Centralized
- IDPS
- ECU 1
- ECU n

### Distributed
- IDPS
- ECU 1
- IDPS
- ECU n

- Reporter – Manages reports from multiple IDPS hosts

### Monitoring
- Network Traffic
- IDPS
- Networking Stack
- APP 1
- APP n

### Inline
- Network Traffic
- IDPS
- Networking Stack
- APP 1
- APP n

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
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
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

---

Summary