**Ironclad perimeter cybersecurity protection**

**Perimeter and CAN bus vulnerabilities**

As vehicles become more connected, they become increasingly vulnerable to malicious attacks. Two major ‘weak spots’ vulnerable to cyber-attacks are the perimeter and the controller area network (CAN) bus.

Attackers may attempt to exploit these ‘weak spots’ by (1) carrying out an intrusion through the perimeter; and (2) using the network to attack remote devices, disrupt network activity, or even attack the network itself.

**Protection from potential attack vectors in the CAN bus**

We can assume that perimeter components will be hacked. Therefore, we strive to fortify the CAN bus and vehicle systems from the potentially compromised perimeter components.

A joint task force has identified CAN bus-related attack vectors in perimeter devices. The task force has proposed a joint solution which enables OEMs to leverage both software and hardware security capabilities to cover potential attack vectors.

**C2A and NXP joint solution**

This joint solution incorporates the following elements:

* NXP's Secure CAN Transceiver for a vehicle's CAN bus
* C2A’s Stamper, a decentralized firewall for the CAN bus
* C2A’s SecMon, a network intrusion detection and prevention system (IDPS)

The joint solution enables effective protection by detecting and preventing potential incidents, as well as providing detailed reports of all kinds of perimeter-related CAN bus cyber-attacks:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Sending out of context data | Tampering with CAN data | Spoofed CAN message by local host | Spoofed CAN message by remote host | Flooding Transmission |
| Detection of incident | V | V | V | V | V |
| Prevention of incident | V | V | V | V | V |
| Origin of incident | V | V | V | V | V |
| Time of incident | V | V | V | V | V |