Securing Ethernet in the car

Using IEEE 802.1 and related standards

Threat analysis, what’s different about the car, network assumptions; traffic segregation, resource segregation; authentication, enrollment, and authorization—who, what, and where; message integrity and authenticity; trusted, untrusted, and vulnerable components; fixed and redundant configuration; bandwidth allocation.
Threat analysis

- Wide range of network attached devices
  - Accident/error/misuse as much of a problem as malice

- Recipients and resources require protection
  - Authenticity and integrity of communication
  - Authorized resource use (resource creation & control)

- Network access/exposure varies across net
  - Open, Normally accessible, Intentionally closed

- Vulnerability
  - Cost/benefit to attacker inc. alternative attack vectors
  - Reputational risk (new technology)
What’s different about the car

- **Small, simple network**
  - Actual network designs vary
  - Coexistence with existing network(s)/bus(es) for some time
  - Small number of flows

- **Network configuration can be/is fixed**
  - At least while car is in operation
  - Fixed filtering/forwarding tables, perhaps by initial build
    - In Normally accessible, Intentionally closed (not Open) components
    - Attached device addresses (changed to) match
  - Fixed resource allocation

- **Repair by halting car**
  - No running repair
  - Can require Internet access to car manufacturer’s central database and record for this car
Network assumptions

- Central controller(s) supporting authentication/enrollment
- External communication through/mediated by central controller
- Producer/consumer relationship for many information flows
Traffic & resource segregation

- Traffic segregation by VLAN
- Asymmetric VLANs support information producer/consumer relationship
Enrollment–adding/replacing a component

- **Locate & authenticate the component/device**
  - VLAN tag enrollment protocol packets
  - Use .1AR IDevID (protocol choices), is it what it claims to be?
  - Has it been stolen/salvaged/traded?

- **Authorize**
  - Does it belong in this car (configuration)

- **Add to centralized database for this car**
  - Has to be a reliable record of everything attached to the car network

- **Provision the component**
  - Install .1AR LDevID
  - Pair-wise MACsec CAK calculated for in-car Authenticator/Key Server – component CA (Secure Connectivity Association)
  - Key Server distributes CAKs for the component’s other CAs
Message Integrity and Authenticity

- Protected by MACsec where vulnerable
  - Particularly in Open locations e.g. trailer hitch
- Perhaps not if physically inaccessible
  - But see ‘reputational risk’
- MACsec protection may be multi-hop
  - As for Customer Bridge to Customer Bridge over provider network (see 802.1AEcg)
  - Where resource protection en-route not important
Reliability, redundancy

- Existing car networks/buses will persist
- May be less redundancy than we might expect
  - Get to the side of the road/limp home adequate
- Duplication/elimination possible
  - Even in simple network designs
  - Qca like MRTs without the need for protocol
  - Multi-hop MACsec can provide elimination w/o extra protocol and has secure supervisory protocol
Bandwidth allocation

- Asynchronous approach highly desirable
  - Node to node time sync along path requires transitive trust