SAE INTERNATIONAL

Advance to the Next Level of Mobility

As the mobility environment becomes more complex and time-to-market pressures rise, there's only one place you can access the latest trends, professional development, and knowledgeable contacts you need to overcome today's mobility challenges and those yet to arrive: 2023 WCX™ SAE World Congress Experience.

Register todayat sae.org/wcx

Cybersecurity Vulnerabilities for Off-Board Commercial Vehicle Diagnostic Sessions

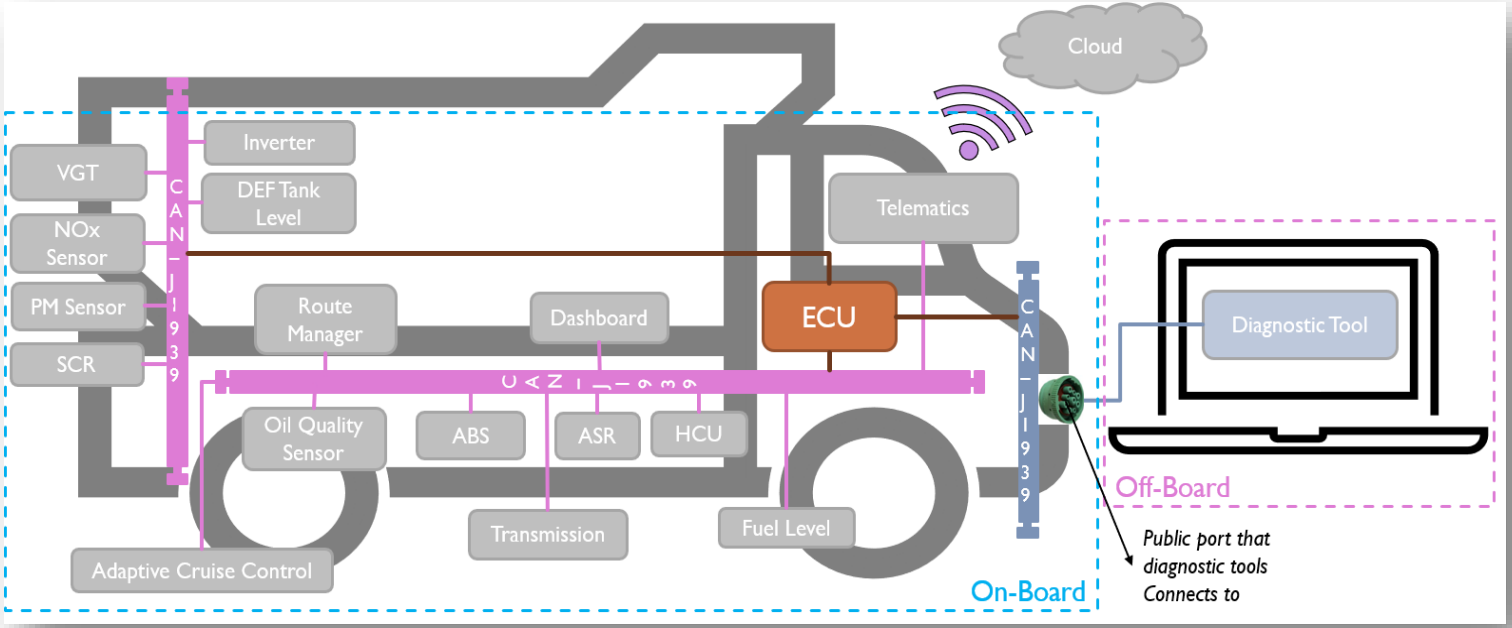
Author(s): Sharika Kumar, Jeremy Daily, Qadeer Ahmed, Anish Arora

Affiliated: Accelera by Cummins/Ohio State University, Colorado State University, Ohio State University

accelera by Cummins

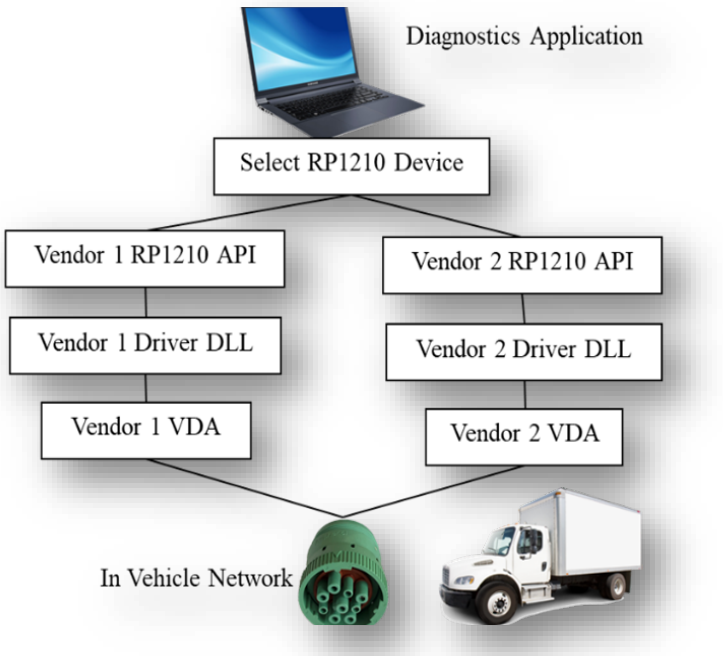
Background: Medium and Heavy Duty (MHD) Network Communication

- MHD networks are typically built on SAE J1939 over CAN 2.0b (Multi-master serial bus, features unicast and broadcast messages, transport fragmentation/reassembly)
- Diagnostic application often run on a Windows-based PC or laptop



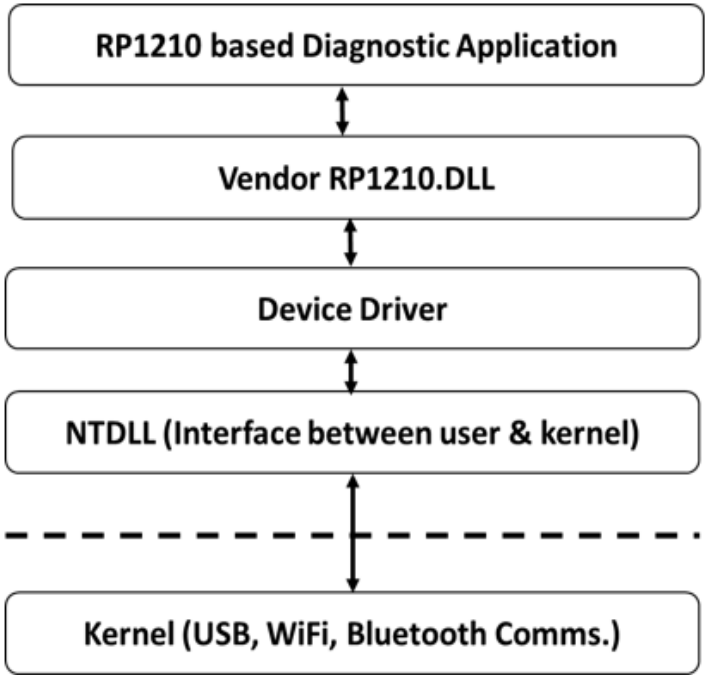
Vehicle Diagnostic Adapters (VDAs)

- VDAs translates vehicle communications to a diagnostic application
- American Trucking Association's (ATA) Technology and Maintenance Council (TMC) initiated RP1210 in the 1990's to manage VDAs
- RP1210 describes a standard API for a Windows PC application to communicate with the network
- A trusted maintenance technician is often granted access to connect a VDA to the diagnostic port to exercise the off-board communications

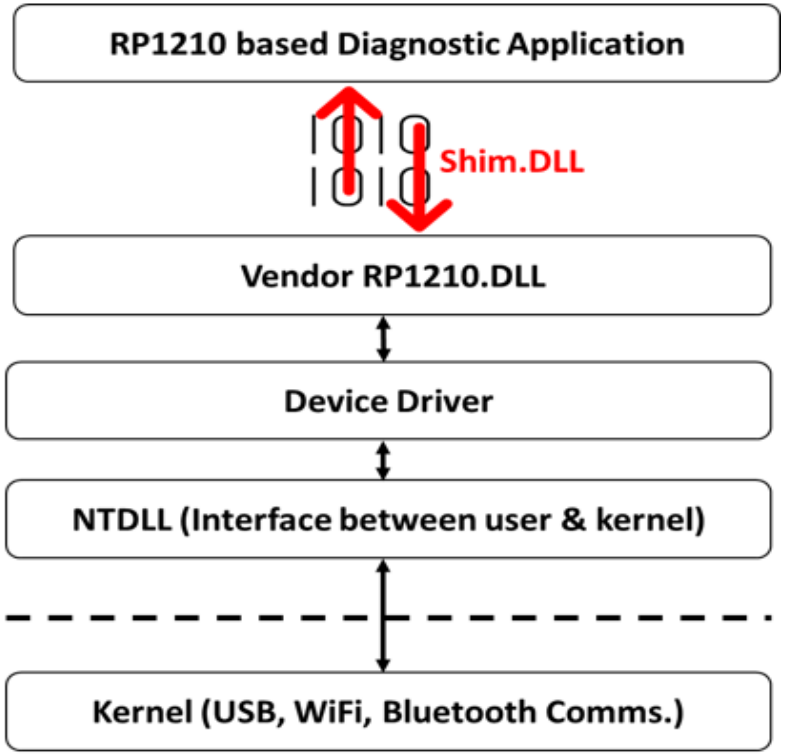


The concept of RP1210

Attacking Vehicle Diagnostic Adapter Drivers

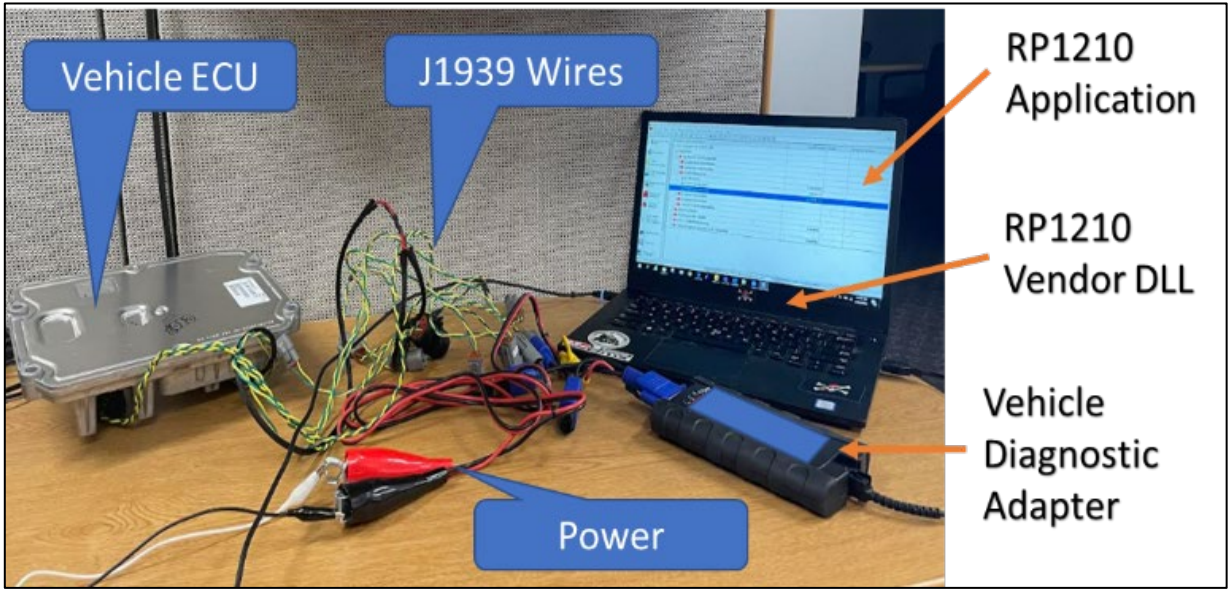


Communication stack within the PC/laptop



Attack uses inserted shim DLL to tamper RP1210 communications

Security Experiment Setup

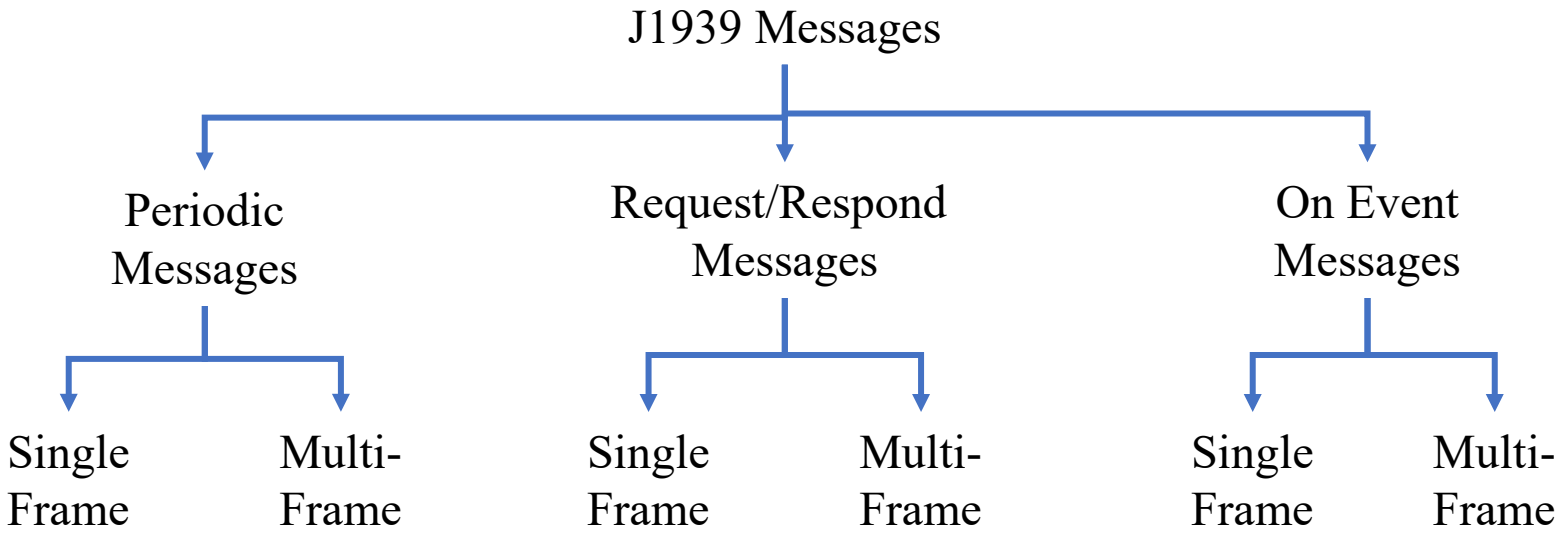


Test Bench with single ECU connected to a diagnostic tool

SAE J1939 Messages and RP1210

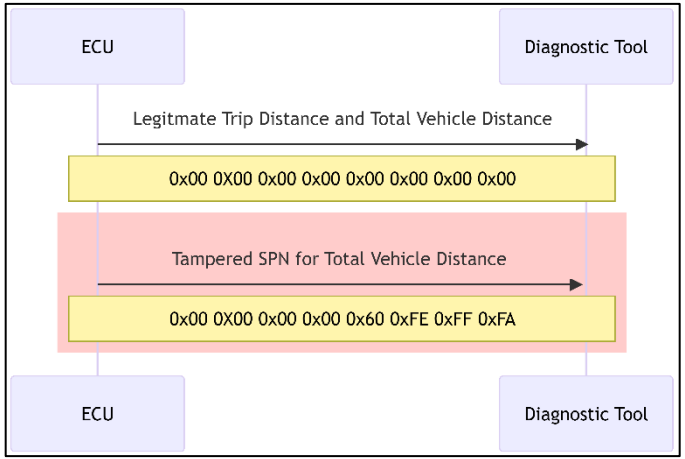
- SAE J1939 messages are typically 8 bytes long due to CAN 2.0b limitation
- SAE J1939-21 TP enables handling messages of length 9-1785 bytes using multiple frames
- Construction/Deconstruction of longer messages can be configured to be handled by RP1210 device driver
- The Parameter Group Number (PGN) data field parameter placement notations and conventions known as Suspect Parameter Number (SPNs) are specified in SAE J1939-71 Vehicle Application Layer published in the SAE J1939-DA

SAE J1939 Message Categorization based on Occurrence Characteristics



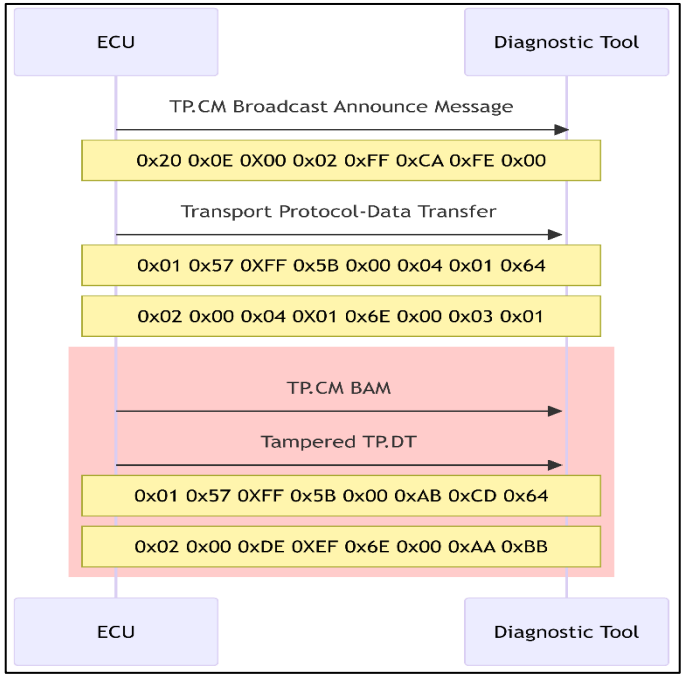
Taxonomy of J1939 messages used

Periodic, Single Frame Message Attack



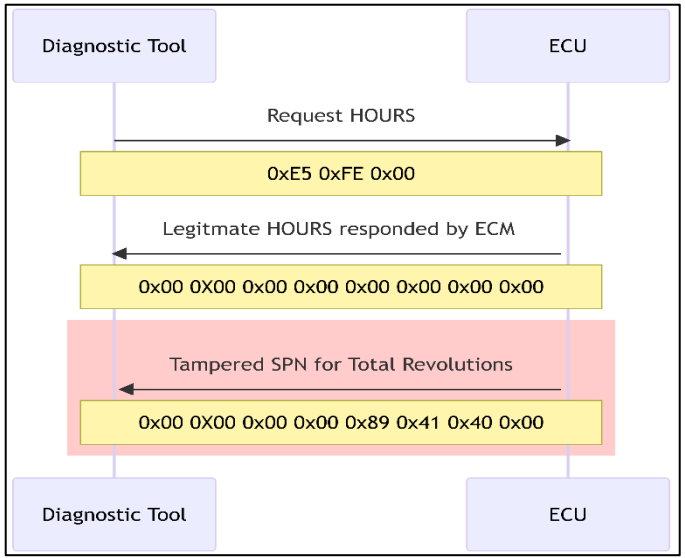
Manipulation of SPN 245, total vehicle distance. The legitimate message has all zeros as the ECM used was brand new

Periodic, Multi-Frame Message Attack



Demonstration of manipulating multi-frame messages in J1939 with the DM1 message as an example.

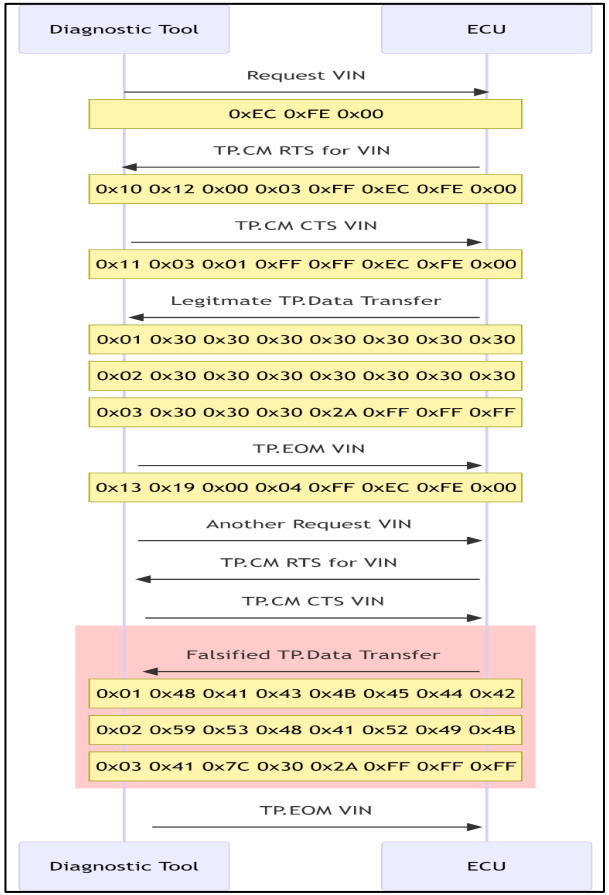
Request/Respond Single Frame Message Attack



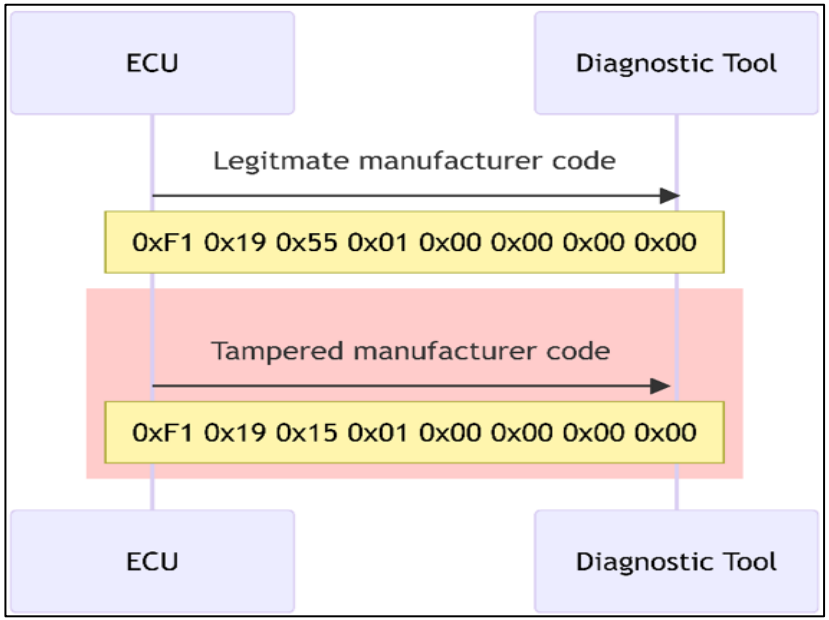
Manipulation an on-request message for engine revolutions. The legitimate message has all zeros as the ECM used was brand new.

Request/Respond Single and Multi-Frame Message Attack

Manipulation of Vehicle Identification Number (VIN), which is a requested multi-frame message.



On-Event Message Attack



Sequence diagram that reflects log files to change the data in the Address Claim in the NAME field defined in SAE J1939-81.

Cyber Defense for Diagnostic Interfaces

Mitigating undetected message manipulation

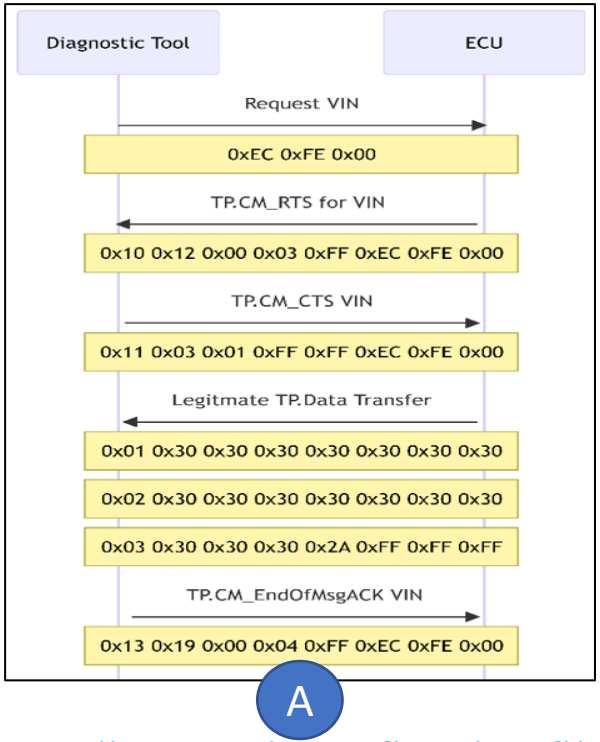
- Security aspect that is compromised is integrity and confidentiality of SAE J1939 messages
- The basic idea of our defense proposal is to transmit a security validation message that the receiver can use to verify if the legitimate message is tampered with or not
- The receiver can simply discard the received frame if verification fails
- In the simplest form the security message could contain a MAC of the freshest or latest message transmitted out

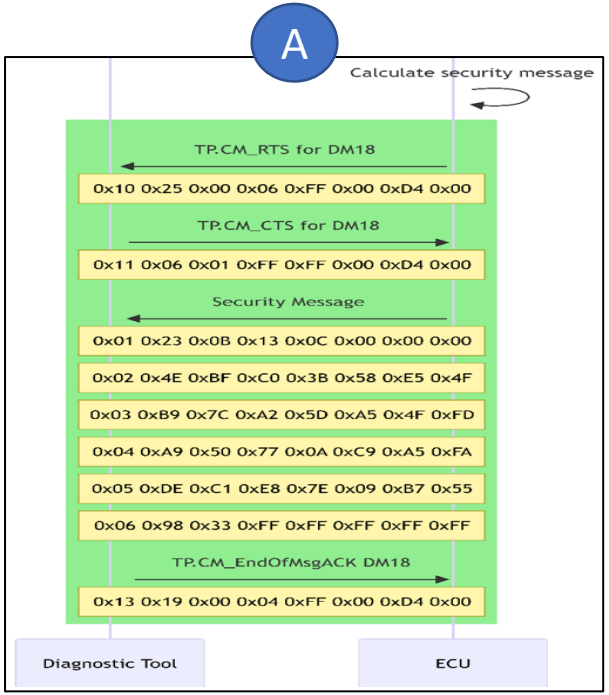
Cyber Defense for Diagnostic Interfaces

Byte Pos.	Bits	Definition (Existing in the SAE J1939-73)	Updates to existing definition
1	8-1(LSB)	Security Entity Length – Length of the data security parameter	
2	8-5(MSB)		
2	4-1	Security Entity Type – Indicating type of usage 0000 – Data is long seed 0001 – Data is long key 0010 – Data is a session key 0011 – Data is a certificate 0100 – 1111 - Reserved	1000 – Data is encrypted with pre-shared key 1001 – Data is signed with pre-shared key 1011 – Data is encrypted and signed with pre-shared key 1100 – Data is encrypted with dynamically derived key 1101 – Data is signed with dynamically derived key 1111 – Data is encrypted and signed with dynamically derived key
3	8-1	Data Security Parameter	Signature/Encryption Calculation – Contains an algorithm identifier
4-5	8-1		Signature Length – Length of signature portion of the message
6-7	8-1		Anti-replay Counter – Incrementing counter to prevent replay attack
8- n*	8-1		Message/Cipher
n+1 – m** n+ Signature Length	8-1		Signature

Data Security Message (Dm18) Updates for Defense

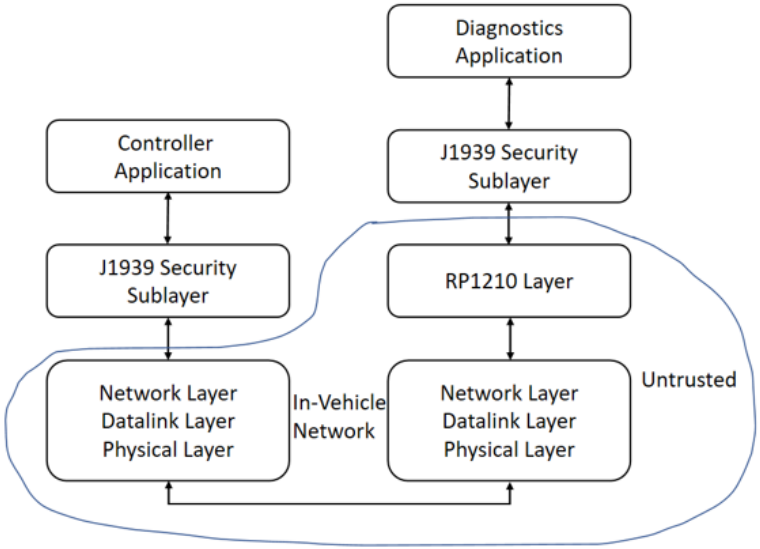
Cyber Defense using DM18





Sequence diagram that reflect log files showing the utility of DM18 to send secure messages over SAE J1939

Cyber Defense for Diagnostic Interfaces



Proposed security architecture were external layers are untrusted

Contributions

- We demonstrate how to inject Machine-in-the-Middle (MitM) attacks on SAE J1939 vehicular communications
- We develop MitM methods to compromise diagnostic tool services
- We also demonstrate holistic mitigation is feasible by architecting a trusted security sublayer that mitigates undetected message manipulations

Contact Info

- Thank you

  - Sharika Kumar
  - Accelera by Cummins and Ohio State University
  - 7018 Stoney Ridge Drive, Columbus, IN -47201
  - +1-812-341-0190
  - kumar.918@buckeyemail.osu.edu
  - sharika.kumar@cummins.com
  - sharikakkumar@gmail.com