Abuse of privileges by staff (insider attack)

Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)

Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)

Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on

Abuse of privileges by staff (insider attack)

Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers

Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)

Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)

Information breach by unintended sharing of data (e.g. admin errors)

Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)

Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)

Communications channels permit code injection, for example tampered software binary might be injected into the communication stream

Communications channels permit manipulate of vehicle held data/code

Communications channels permit overwrite of vehicle held data/code

Communications channels permit erasure of vehicle held data/code

Communications channels permit introduction of data/code to the vehicle (write data code)

Accepting information from an unreliable or untrusted source

Man in the middle attack/ session hijacking

Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway

Interception of information / interfering radiations / monitoring communications

Gaining unauthorized access to files or data

Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner

Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles

An unprivileged user is able to gain privileged access, for example root access

Virus embedded in communication media infects vehicle systems

Malicious internal (e.g. CAN) messages

Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)

Malicious diagnostic messages

Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)

Compromise of over the air software update procedures. This includes fabricating the system update program or firmware

Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware

The software is manipulated before the update process (and is therefore corrupted), although the update process is intact

Compromise of cryptographic keys of the software provider to allow invalid update

Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features

Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack

Defined security procedures are not followed

Manipulation of functions designed to remotely operate systems, such as remote key, immobilizer, and charging pile

Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)

Interference with short range wireless systems or sensors

Corrupted applications, or those with poor software security, used as a method to attack vehicle systems

External interfaces such as USB or other ports used as a point of attack, for example through code injection

Media infected with a virus connected to a vehicle system

Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)

Extraction of copyright or proprietary software from vehicle systems (product piracy)

Unauthorized access to the owner’s privacy information such as personal identity, payment account information, address book information, location information, vehicle’s electronic ID, etc.

Extraction of cryptographic keys

Illegal/unauthorized changes to vehicle’s electronic ID

Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend

Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)

Data manipulation to falsify vehicle’s driving data (e.g. mileage, driving speed, driving directions, etc.)

Unauthorized changes to system diagnostic data

Unauthorized deletion/manipulation of system event logs

Introduce malicious software or malicious software activity

Fabrication of software of the vehicle control system or information system

Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging

Unauthorized access of falsify the configuration parameters of vehicle’s key functions, such as brake data, airbag deployed threshold, etc.

Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.

Combination of short encryption keys and long period of validity enables attacker to break encryption

Insufficient use of cryptographic algorithms to protect sensitive systems

Using already or soon to be deprecated cryptographic algorithms

Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack

Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present

Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges

Superfluous internet ports left open, providing access to network systems

Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages

Information breach. Personal data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)

Manipulation of electronic hardware, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack