old ID	Category of threat	sub-category	Example of vulnerability or attack methodology	Comments from ITU-T SG17
1	Compromise of back-end server	Server used to attack vehicle	Abuse of privileges by staff (**insider attack**)	
			Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL	
			Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	
		Services from back-end server disrupted	**Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on.	
1		Data held lost/ compromised	Abuse of privileges by staff (**insider attack)**	
2			**Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when stored by third-party cloud service providers	
			Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	
			Unauthorised physical access to the server (conducted for example by USB sticks or other media connecting to the server)	
38			**Information leakage** or sharing (e.g. admin errors, storing data in servers in garages)	
15	Communication channels used to attack a vehicle	Spoofing	**Spoofing of messages** (e.g. 802.11p V2X during platooning, etc.) by impersonation	
			Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	Propose to add "Sybil attack" under Spoofing
21		Communication permits tampering with vehicle held code/data	**Code injection**, for example tampered software binary might be injected into the communication stream	
			Manipulate data/code	
			Overwrite data/code	
			Erase data/code	
			Introduce (write data code)	
20		Repudiation	Accepting information from an **unreliable or untrusted source**	This sub-category would be better to be changed from '**Repudiation**' to '**Attack on integrity/Data trust**'
16			**Man in the middle** / session hijacking.	
18			**Replay attack**, for example against communication gateway allows attacker to downgrade software of ECU or firmware of gateway	
		Information Disclosure	**Interception of information** / interfering radiations / monitoring communications	
			Gaining **unauthorised access** to files or data	

8		Denial of service	**Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner	
		Elevation of privileges	An unprivileged user **gains privileged access**, for example root access	
24		Message types	Malicious **internal** (e.g. CAN) **messages**	"Message types" may not be suitable for this sub-category of threat. This should be "**Message injection**". An addition of example of attack methodology (malicious diagonostic message) is proposed.
25			Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	
			Malicious Diagnostic Message	
25			Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)	
74	Update process used to attack a vehicle	Misuse of updates	Compromise of **software update procedures**, including over-the-air updates. This includes fabricating system update program or firmware	
28		Denying updates	Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features.	
70	Human factor	Abuse of authorisations by owner, operator or engineer	Unauthorised use or **addition of devices or systems**	Human factor may be security threat occurred by **human mistake**. However, '**Abuse of …**' should not be categorized to "Human factor". **How about changing 'Human factor' to something else?**
			Unauthorised use or **manipulation of software**	
77			**Installing unauthorized software**	
44		Misconfiguration	**Misconfiguration of equipment** by maintenance community or owner during installation/repair/use causing unintended consequence	
83			**Erroneous use** or administration of devices and systems (inc. OTA updates)	
46		Unintended actions	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack	
67	Physical manipulation of systems to enable an attack	Physical manipulation of systems to enable an attack	**Manipulation of hardware**, e.g. hardware added to a vehicle to enable "man-in-the-middle" attack	
68	Early stage attack	Early stage attack	**Hardware or software, engineered to enable an attack** or fail to meet design criteria to stop an attack	
79	Compromise of external connectivity	Vehicle functions using connectivity	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobiliser, and charging pile	
88			**Manipulation of telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	
80			Interference with **short range wireless systems** or sensors	
		Hosted 3rd party software e.g. entertainment apps	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems	
81		External interfaces	**External interfaces** such as USB or other ports may be used as a point of attack, for example through code injection …	
89			Overcome **diagnostic access** to manipulate vehicle parameters (directly or indirectly)	
9	Vehicle used as	Attack on other vehicles	Transmission of false/unreliable/contaminated data or **V2V messages to other vehicles**	
			Timing Attack, for example delaying delivery of safety message to other vehicles	It is proposed to add a timing attack as an example.
			Masquerading Attack, for example, a malcious vehicle attempting to act as an emergency vehicle to deceive other vehicles	It is proposed to add a masquerading attack as an example.
			Denial of service, for example flooding other vehicle	It is proposed to add a denial of service as an example.

10	a means to propagate an attack	Attack on external devices connected to a vehicle (e.g. cell phones)	Use of a vehicle as means to **compromise connected devices**	
11		Attack on infrastructure	Transmission of false/unreliable/contaminated data **to infrastructure**	
			Denial of service, for example flooding infrastructure	DoS should be also listed here as an example.
		Attack on network	Vehicle acting as a **botnet**	
			Denial of service, for example flooding network	DoS should be also listed here as an example.
52	Target of an attack on a vehicle	Extract Data/Code	Product **piracy** / stolen software	
61			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.	
63			**Extraction of cryptographic keys**	
53		Manipulate Vehicle Data	Illegal/unauthorised changes to **vehicle's electronic ID**	
56			**Identity fraud.** For example if a user wants to display another identity when communicating with toll systems, manufacturer backend	
54			Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	
62			Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)	
58			Unauthorised changes to **system diagnostic data**	
xx		Erase Data/Code	Unauthorized deletion/manipulation of **system events log**	
72		Introduce malware	Introduce **malicious software** or malicious software activity	
76		Introduce new software or overwrite existing software	**Fabricating software** of the vehicle control system or information system	
		Disrupt systems or operations	**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 malicious payload	
57		Manipulate Vehicle Parameters	Unauthorized access or **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	
60			Unauthorized access or **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.	
90	System design exploits (inadequate design and planning or lack of adaption)	Encryption	Combination of short **encryption keys** and long period of validity enables attacker to break encryption	
XX			Insufficient use of cryptographic algorithms to protect sensitive systems	
94			Using deprecated **cryptographic algorithms** (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software)	
75		Software development	**Software bugs**. The presence of software bugs is a basis for potential exploitable vulnerabilities … software bugs are more likely to happen than Hardware failures over the lifetime of a car	
93			**Using remainders** from development (e.g. debug ports, JTAG ports, development certificates, developer passwords, …) to gain access to ECUs or gain higher privileges	
		Network design	**Default internet ports left open**, providing access to network systems	
92			Circumvent **network separation** to gain control (Truck hijacking)	

33	Data loss from vehicle	Physical loss of data	**Damage** caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	
36			Loss from **DRM** (digital right management) conflicts. User data may be deleted due to DRM issues	
37			The (integrity of) sensitive data may be lost due to IT **components wear and tear**, causing potential cascading issues (in case of key alteration, for example)	
35		Unintended transfer of data	Information leakage. Private or sensitive data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)	
3	Communication loss to/from vehicle	Communication jamming	**Jamming** (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems	
5		Environmental effect	Failures or **disruptions of communications links**, network outage or other systems (e.g. through disruptions of power/main supply)	
		Disruption of communication	**Black hole attack,** in order to disrupt communication between vehicles by blocking of transferring some messages to other vehicle	Black hole attack should be in the list.
			Flooding a huge volume of dummy messages to vehicle or infra to disable to communicate	Flooding should be also listed here.
65	Other	Vehicle - failure	**Failures / malfunctions of (parts of) devices or systems**	
91		Manipulate Data/Code	Elude VIN locks to use **stolen ECUs**	
		Sensor spoofing	**Spoofing of physical effects** which are detectable by sensors e.g. radar signals	
26		Eavesdroping on communication channel	**Gaining private information** (e.g. payment account information, data related with location of vehicle)	It is proposed to add a gaining private information as an example.