**Recommendation
of the Task Force on Cyber Security and Over-the-air issues
of UNECE WP.29 IWG ITS/AD
on Cyber Security**

1. Introduction
	1. A Task Force was established as a subgroup of the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) of WP.29 to address Cyber Security issues, relevant for the automotive industry. The task force consisted of members of the automotive industry and regulators. This is its output.
	2. This paper defines principles/objectives to be obtained to address the key cyber risks and threats in order to assure vehicle safety in case of cyber-attacks. It further defines detailed guidance or measures for how to meet these objectives/principles. This may include processes and technical approaches. Finally it considers what assessments or evidence may be required to demonstrate compliance or type approval with any requirements identified.
	3. Vehicles may have a range of different types of data on them, including vehicle settings, parameters and personal data. The paper additionally defines principles/objectives to be obtained to protect this data from unauthorized access, amendment or deletion both when it is stored and when it is transmitted. The paper does not define how the data should be treated from a privacy perspective but does consider the implications of data protection legislation and privacy legislation within its recommendations.
	4. The paper further defines principles/objectives to be obtained to protect the security of software updates, including over the air updates.
	5. This paper takes into account the document titled “Guideline on cybersecurity and data protection”, developed by the IWG on ITS/AD and other relevant standards, practice(s), directives and regulations concerning cyber security that are applicable to the automotive industry.
	6. The approach adopted for defining the principles and objectives is to use standard risk management principles. The paper identifies key risks and threats concerned with its principles subject areas. It considers how these risks may be manifest and specific examples of how they might affect a vehicle. The list provided is not exhaustive but is highly illustrative of possible cyber threats posed to the automotive industry. The paper then identifies key mitigations that are required to reduce or minimise those risks and recommends further provisions by which the mitigations might be implemented.
	7. The scope of what aspects of a vehicle the paper covers is defined within a reference model. This details the extent of the vehicle ecosystem that the principles and objectives relate to. It further clarifies that the scope of this paper considers the vehicle lifecycle and that it considers mitigations that could be used before, during and after a cyber-attack.
	8. This paper finally provides recommendations on the outputs use. This includes how it may be taken forward as a regulation or a resolution and, where applicable timelines, for delivery. The style of the paper is intended to be written so that it serves as a basis for the development of prescriptions in UN Regulations to ensure cybersecurity and data protection.
2. **Definitions (and abbreviations)**

|  |  |
| --- | --- |
| **Data privacy** |  |
| CAV | Connected and Autonomous Vehicle |
| Cyber Security | The use of technologies, processes and practices designed to protect networks, devices, services and programs – and the information and data on them – from theft, damage, attack or unauthorized access |
| The automotive industry | Manufacturers, suppliers, maintenance providers and providers of systems and services that interact with the vehicles (e.g. back end systems and 3rd party systems |
| Data protection |  |
| Over-The-Air updates |  |

1. **Reference Model**
	1. The CAV Cyber Security reference model (referred to as the ‘reference model’) defines the scope of the CAV ecosystem, including the components and interfaces between them, for which cyber security threats are considered herein. Its final form was informed by the threat analysis outlined in Section IV. Figure III.i illustrates the CAV ecosystem as envisaged in the analysis.



Figure III.i The CAV Ecosystem. This model is a conceptual representation of the CAV ecosystem, and is agnostic of specific physical implementations and technologies, recognizing these will change over time. It can be used as a basis to identify cyber-attack surfaces and vectors.

* 1. The reference model is an abstraction and is solution agnostic, which is illustrated in Figure III.ii below, and incorporates the following:
		1. The CAV, including: its hardware, its software, the data held on the CAV (including personal data), its internal communications, its interfaces with external communication systems (for example V2X and emergency communications) and devices (for example USBs and CDs), CAV functions and systems that use wireless communications (for example tyre pressure monitoring system (TPMS) and keyless entry);
		2. Support servers which directly communicate with the CAV;
		3. Diagnostic/maintenance systems. This includes consideration of Aftermarket Operations, which will have direct access to CAVs and the ability to directly connect to it with its workshop equipment;
		4. The lifecycle of a cyber-attack: “pre-attack” requires consideration of approaches for prevention, “during attack” requires consideration of approaches for detection, and “post attack” requires consideration of approaches for response;
		5. Protecting the CAV throughout its lifecycle from development through to scrappage.
	2. The reference model excludes the following aspects. Whilst these aspects might be targets of some form of attack, other appropriate bodies should consider them.
		1. Data privacy. The reference model does take into account protecting all data (including personal data) held in the CAV ecosystem, however data privacy is excluded as that is considered to be subject to existing and emerging regulations;
		2. Software updates. The reference model does take into account the security of software updates received by the CAV, however how the functionality of legitimate software updates might impact the system or vehicle type approval are the subject of a separate paper;
		3. The interception and manipulation of messages transmitted from the CAV. The reference model does reflect that messages generated and transmitted by the vehicle must be accurate and appropriately protected, however whatever receives the message should still take measures to ensure the received message was as intended;
		4. Attack actions on the communication medium between the vehicle and the external device, for example causing disruption of the communications channel, jamming or spoofing of physical signals;
		5. Third party devices. It is recognised that manufacturers cannot control all devices that might be connected to it, for example those inserted into the on board diagnostics port. Where controls can be applied is at the connecting interfaces for these devices.



Figure III.ii The CAV Cyber Security Reference Model.

1. **Threat Analysis**
	1. The process of threat analysis started with the identification of various threats. A list of threats was identified. This list provides a number of theoretically possible examples of vulnerabilities or attacks that may be conducted against automotive vehicles, including their connected ecosystem.
	2. Attack versus Vulnerability
	3. The threats were categorized as attacks or vulnerabilities, based on how it was manifested on the vehicle. Vulnerabilities were considered as system (vehicle) security shortcomings that would be exploited by an external entity. Attacks were considered as the mode of operation of the external entity which exploits the security vulnerabilities of the system (vehicle).
	4. Threat Effect
	5. Threat effects were identified from an attacker point of view in terms of where the attack is performed. If the attack is performed on an asset where there is an imminent effect on the asset, then is classified as direct, e.g. compromising an OEM back end server and stopping it from functioning.
	6. However if the attack impacts multiple assets beyond the ones on which it is performed, it is classified as cascading, e.g. compromising an OEM back end server and sending malicious proprietary messages to the vehicle, thereby affecting both the OEM backend server and the vehicle.
	7. A classification of threat effects were done in order to better identify the mitigation measures ( Section VI): Cascading threats will always have an associated direct threat as a root cause, which can help in sequential identification of the threat effects and corresponding mitigation measures
	8. Access Method
	9. The column “Access Method” can be used to clarify how the threat is propagated within the vehicle subnetwork.  “Access method” have the following subdivisions:
* Physical (Malicious diagnostic messages, Attack via USB, ODB-2 port etc.)
* Remote (Back end server attack, malicious V2X messages, compromising OTA update etc.)
* Threat Path (gives additional information as to how the identified attacks may propagate to the vehicle sub network)
	1. Threat Path is further classified into:
* **Single–hop** threat path can be attributed to those threats where the attacker directly interacts with the vehicular network, e.g. Attacks which is facilitated via direct connection through telematics unit (OBD-2/ USB).
* **Multi- hop** threat path can be considered where the attack perpetuates through more than one networks before impacting the vehicle sub network, e.g. compromising an OEM back end server and sending malicious proprietary messages to the vehicle, where the attacker first gets into the OEM backend server network and then impacts the vehicular network.
	1. Vehicle architecture
	2. The next phase in the threat analysis process was to identify the areas within the vehicle architecture where the attack could have an impact. Since it is practically impossible to list down each and every point of attack in the vehicle, a high level vehicle architecture was identified with the following elements:
* **External architecture-** This refers to elements that are present outside (remote location) the vehicle through which an attack can be manifested affecting the vehicle ecosystem.
* **Wireless Architecture-** This includes elements that are part of the vehicle interface which provides a connection (and an attack path) to the outside world via wireless means.
* **Physical Architecture-** This includes elements that are part of the vehicle interface which provides a connection (and an attack path) to the outside world via physical means.
* **Internal Architecture**- This includes elements that are present within the vehicle internal architecture which affects the actual operation/ behavior of vehicular functions.
	1. The below diagram provides a comprehensive overview of these elements and how they fit within the vehicle architecture.



* 1. The vehicle architecture is used to identify where the attack can have its effect. It is also used to showcase how the attack may propagate through the system. A numbering scheme (with 1 being the entry point) is used to show where the attack will initially affect the vehicle ecosystem and how it will affect subsequent systems. An example would be for “denial of service (ID 22)” (threat matrix document reference). Here the attack may occur via any of the physical, wireless or external interfaces (although some are more likely than others). So they all have been annotated “1” as a potential entry point. If propagated the attack might then enter either the Infotainment Network or the Wider Vehicular Network (both designated “2”). From there it could in theory go through a gateway to the ECU network, onto that network and then to an ECU. Hence the respective scores of 3, 4 and 5.
	2. Where the table lists the target of an attack or a vulnerability, the method of following a potential attack through a system does not necessarily fit well. For these rows an alternative approach of merely identifying which assets might be affected was taken. The assets are marked with an “x”. An example is the target of an attack being “Erase data/code”. For this the attack it is assumed that data/code is only held within the vehicle architecture. So these entries (elements) which may affect the have been marked.
	3. Attack outcome
	4. The final part of the threat analysis process was to identify the attack outcomes and how it can be used to identify cybersecurity principles (section V) and mitigations measures (section VI). Attack outcomes were generally classified into the following types:
1. Safe operation of vehicle affected
2. Vehicle functions stop working
3. Software modified, performance altered
4. Software altered but no operational effects
5. Data integrity breach
6. Data confidentiality breach
7. Other, including criminality
	1. For each of the identified attacks/ threats, the corresponding outcome is marked in the threat matrix with an ‘x’ mark.

**Attack categories and sub categories**

|  |  |
| --- | --- |
| Category of threat | Sub Category |
| Compromise of back-end server | Server used to attack vehicle |
| Services from back-end server disrupted |
| Data held lost "data leakage" / compromised |
| Communication channels used to attack a vehicle | Spoofing |
| Communication permits tampering with vehicle held code/data |
| Attack on Integrity / Data Trust |
| Information Disclosure (including eavesdropping) |
| Denial of service |
| Elevation of privileges |
| Virus infection |
| Message injection / tampering |
| Update process used to attack a vehicle | Misuse of updates |
| Denying updates |
| Human factor and social engineering | Misconfiguration |
| Unintended actions |
| Compromise of external connectivity | Vehicle functions using connectivity |
| Hosted 3rd party software e.g. entertainment apps |
| External interfaces |
| Target of an attack on a vehicle | Extract Data/Code |
| Manipulate Vehicle Data |
| Erase Data/Code |
| Introduce malware |
| Introduce new software or overwrite existing software |
| Disrupt systems or operations |
| Manipulate Vehicle Parameters |
| System design exploits (inadequate design and planning or lack of adaption) | Encryption |
| Early stage attack |
| Software and hardware development |
| Network design |
| Data loss / "data leakage" from vehicle | Physical loss of data |
| Unintended transfer of data |
| Physical manipulation of systems to enable an attack  | Physical manipulation of systems to enable an attack |
| Vehicle used as a means to propagate an attack*(Category agreed as out of scope due to vehicle needing to be compromised first)* | Attack on other vehicles |
| Attack on external devices connected to a vehicle (e.g. cell phones) |
| Attack on infrastructure |
| Attack on network |
| Communication loss to/from vehicle *(potentially out of scope as not cyber security)* | Communication jamming |
| Environmental effect |
|  Non-cyber security vehicle threats *(potentially out of scope)* | Vehicle - failure |
| Manipulate Data/Code |
| Sensor spoofing |

* 1. A detailed description of all the threats and corresponding mitigation measures can be found in Annex 1 of this document.
1. **Cyber security principles**
	1. Review and identification of cyber security principles (ITS/AD and UK DfT principles
2. **Mitigations for cyber security**
	1. A list of mitigations were identified. These provide one or more ways that the threat examples identified could be mitigated. A number of reference documents were used to identify these mitigations, these are provided in Annex 2. There is a many to many relationship between threats and mitigation measures. For each threat example a number of mitigations may be applied, similarly one mitigation measure can be used to mitigate more than one threat.
	2. The “Extended CIA” (Confidentiality, Integrity, and Availability) approach can be used as a method to identify mitigations. The following protection objectives are defined under the “Extended CIA “approach:
	3. The mitigations identified are provided at two levels. The first provides security controls that need to be implemented. The second level provide more detailed measures that could, either individually, collectively or through use of some of them, provide methods of implementing the security control. The second level is not intended to be exhaustive, other additional measures could also be applied.

An example of this approach would be the security control:

 *“Access control techniques and designs shall be applied to protect system data/code”*

Possible recommendations that can be included under the above security control would be:

* Application based input validation (in terms of what kind of data/input the affected application is expecting)
* Secure storage of sensitive information
* Access control and read/write procedures established for vehicle files and data
* Network segmentation and implementation of trust boundaries
* System monitoring
* Software testing
* Active memory protection
	1. The mitigations that shall be applied are:
1. Security Controls shall be applied to back-end systems to minimize the risk of insider attack
2. Security Controls shall be applied to back-end systems to minimize unauthorized access
3. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage
4. Security Controls shall be applied to minimize risks associated with cloud computing
5. Security Controls shall be applied to back-end systems to prevent data leakage
6. Systems shall implement security by design to minimize risks
7. Access control techniques and designs shall be applied to protect system data/code
8. Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data
9. Measures to prevent and detect unauthorized access are employed
10. Messages processed by a receiving vehicle shall be authenticated and integrity protected
11. Cybersecurity best practices shall be followed for storing private keys
12. Confidential data transmitted to or from the vehicle shall be protected
13. Measures to detect and recover from a denial of service attack shall be employed
14. Measures to protect systems against embedded viruses/malware are recommended
15. Measures to detect malicious internal messages are recommended
16. Secure software update procedures are employed
17. Cybersecurity best practices shall be followed for defining and controlling maintenance procedures
18. Cybersecurity best practices shall be followed for defining and controlling user roles and access privileges
19. Organizations shall ensure security procedures are defined and followed
20. Security controls are applied to systems that have remote access
21. Software shall be security assessed, authenticated and integrity protected
22. Security controls are applied to external interfaces
23. Cybersecurity best practices for software and hardware development shall be followed
24. Data protection best practices shall be followed for storing private and sensitive data
25. Systems should be designed to be resilient to attacks and respond appropriately when its defenses or sensors fail
	1. A detailed description of all the security controls, with their associated detailed measures that could be used to implement them, can be found in Appendix 3.
26. **Conclusion and Recommendation for further proceedings**
* to ITS/AD
* on General approach (Guideline vs. Regulation, etc.)
* Ensure those potential targets of cyber-attacks that are excluded from the reference model are adopted by the appropriate bodies.
* How to do compliance

**Annex 1: List of threats and corresponding principles and mitigations**

**Annex 2: List of reference documents**

* 1. The following list contains references to documents that were drawn upon and used in the creation of this paper:
* ENISA report “Cyber Security and Resilience of Smart Cars” TFCS-03-09
* UK DfT Cyber Security principles TFCS-03-07
* NHTSA Cyber Security Guideline TFCS-03-08
* IPA “Approaches for Vehicle Information Security” (Japan) TFCS-04-05
* UNECE Cyber security guideline (ITS/AD) WP.29/2017/46
* SAE J 3061
* ISO 19790
* ISO 26262
* US Auto ISAC (report by Booz Allen Hamilton) <https://www.automotiveisac.com/best-practices/>
* ISO 19790 “Security requirements for cryptographic modules”
* GSMA CLP.11 IoT security guidelines and CLP.17 IoT Security Assessment

**Annex 3: List of mitigations incl. examples** *(based on Part 2 of TFCS-07-04, further description might be necessary*