International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1371

(05/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent transportation system (ITS) security

Security threats to connected vehicles

Recommendation ITU-T X.1371

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1389**
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1371

Security threats to connected vehicles

Summary

Recommendation ITU-T X.1371 describes security threats to connected vehicles and the vehicle eco-system.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1371	2020-05-29	17	11.1002/1000/14090

Keywords

Connected vehicle, security threat.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1371

Security threats to connected vehicles

1 Scope

This Recommendation describes security threats to connected vehicles. This Recommendation could be referenced in future ITU-T Recommendations to ensure that they consistently take into account the security aspects of intelligent transport systems (ITSs).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.2 confidentiality [b-ITU-T X.800]: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.3 integrity [b- ISO/IEC 27000]: Property of accuracy and completeness.

3.1.4 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
ADAS	Advanced Driver Assistance System
CAN	Controller Area Network
CAM	Cooperative Awareness Message
C-V2X	Cellular-based Vehicle-to-X

DENM	Decentralized Environmental Notification Message
DRM	Digital Rights Management
DSRC	Dedicated Short-Range Communication
ECU	Electronic Control Unit
GNSS	Global Navigation Satellite System
ICT	Information and Communication Technology
ID	Identifier
IT	Information Technology
ITS	Intelligent Transport System
IVN	In-Vehicle Network
JTAG	Joint Test Action Group
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
OBD	On-Board Diagnostic
ODR	Operating Data Recorder
OEM	Original Equipment Manufacturer
OTA	Over The Air
RF	Radio Frequency
RSU	Roadside Unit
SD	Secure Digital
SQL	Structured Query Language
USB	Universal Serial Bus
V2D	Vehicle-to-nomadic Device
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VIN	Vehicle Identification Number
Wi-Fi	Wireless Fidelity

5 Conventions

None.

6 Model of connected vehicle (vehicle ecosystem)

Figure 1 shows the concept of a connected vehicle and its ecosystem. This model is a conceptual representation of the vehicle ecosystem, and is agnostic of specific physical implementations and technologies, recognizing that these will change over time. The model may not capture all technologies or systems used in a vehicle ecosystem but can be used as a basis to identify security threats.

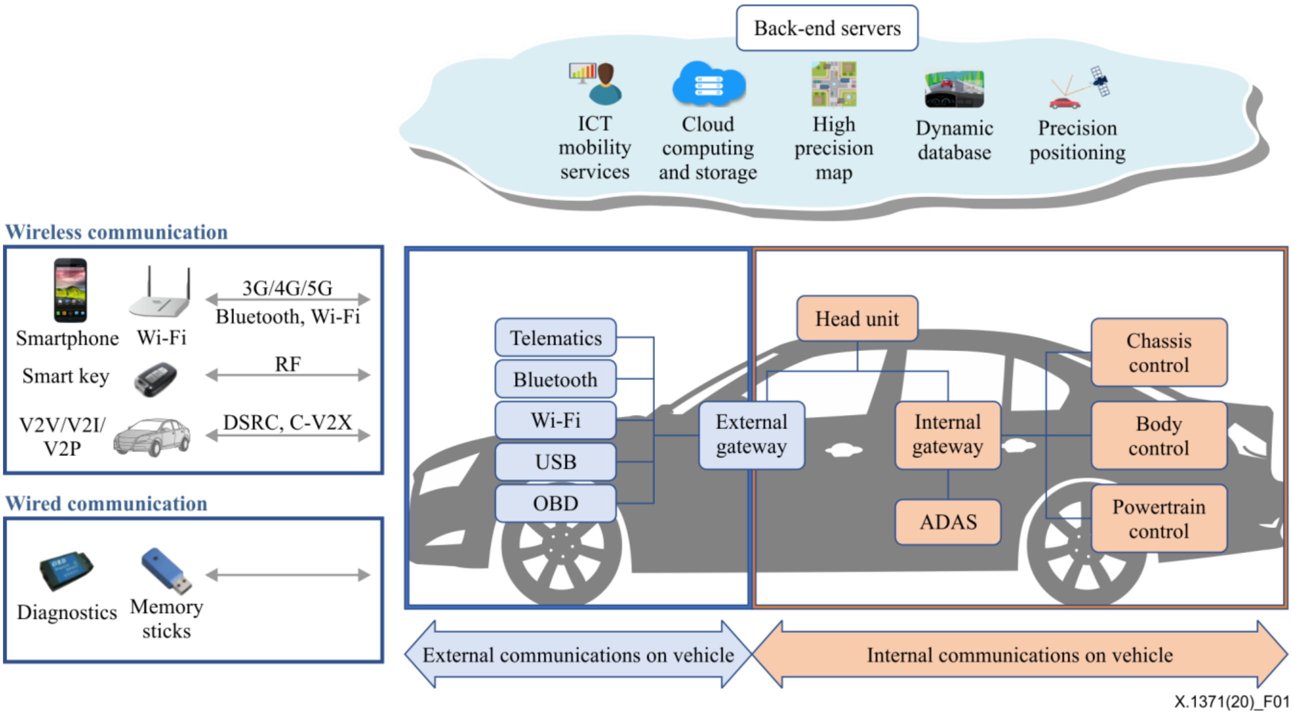

Figure 1 – A concept of connected vehicle (vehicle ecosystem)

Nowadays, communication technology plays an important role in vehicles. Vehicular communication can be classified into that which is external and internal to a vehicle. The internal network of a vehicle, known as the in-vehicle network (IVN), involves vehicle components such as sensors and electronic control units (ECUs). These sensors and ECUs are used in several domains such as chassis control, body control and powertrain control of the vehicle. Moreover, these components are used in an advanced driver assistance system (ADAS), which supports a driver while driving, e.g., in keeping driving lane and cruise control functionality. The head unit is a component of automotive infotainment, which gives the user control over the vehicle's information and entertainment media, e.g., audio and video.

The external communications of a vehicle are called V2X, which stands for "vehicle-to-everything" where "everything" is anything relevant to the vehicle's safe and efficient operation. In particular, V2X is used as a generic term for communication modes such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic device (V2D) and vehicle-to-pedestrian (V2P). V2X technology includes dedicated short-range communication (DSRC) and cellular-based V2X (C-V2X). The infrastructure consists of roadside units (RSUs) and backend facilities, e.g., traffic management and monitoring systems. The RSUs can be connected to the backend facilities through wire or wireless networks. Figure 1 shows various functions in the backend servers. It includes information and communication technology (ICT) mobility services, cloud storages, high-definition map, a dynamic database for neighbouring environment and precision positioning of the vehicle.

External and internal gateways in Figure 1 play a role in addressing the complexity of vehicular communication. The internal gateway handles data in the in-vehicle domain. The external gateway is responsible for communication between the vehicle and external devices, e.g. smartphones and other vehicles, through V2X communication technology. External communication can be categorized as wired and wireless communication. Wired communication can use an on-board diagnostic II (OBD II) port to communicate with diagnostic devices and vehicle software or firmware updates. The wireless communication channel includes cellular communication technology, Wi-Fi and Bluetooth to connect a vehicle with mobile devices such as smartphones.

7 Threats to connected vehicles or vehicle ecosystem and potential information related to threats

7.1 Threats to connected vehicles or vehicle ecosystem

7.1.1 Threats regarding backend servers

In recent years, diversification of connectivity in vehicles has increased remarkably, and in particular, connectivity with various servers (called "backend servers") located at the backend of vehicles is highly required. Backend servers include those provided by original equipment manufacturers (OEMs), suppliers and ICT services to support the vehicle ecosystem from the remote backend.

7.1.1.1 Backend servers used as a means to attack a vehicle or extract data

In a vehicle ecosystem, the backend server mainly collects data from the vehicle, stores it, and sends information to the vehicle. The following threats to the backend server should be addressed to prevent it from being comprised by an unauthorized entity.

– Authority abuse by insider: Abuse of insider's administrative privileges on the backend server may reveal data leakage from the server, send false information to the vehicle, etc.

– Unauthorized access from outside to a backend server: If there remains back-door or known vulnerability in the backend server, it can be exploited from the outside to attack the backend server by means of attack methods such as structured query language (SQL) injection and malware injection. If the attacker obtains the administrative privileges of the server, the same damage as that described in the previous entry should also be considered.

– Unauthorized physical access: There are several ways to physically access the backend server, e.g., using a universal serial bus (USB) flash drive or entering the server's building by using a spoofed staff identifier (ID). In this case, damage and interference to the vehicle-related data and its information-processing facilities are even greater.

7.1.1.2 Backend server service disruption

Attacks on the backend server can cause it to malfunction, disrupt its interaction with vehicles and the provision of services on which vehicles rely. Attacks may cause severe harmful impact on the availability of vehicle-related services, e.g., certification management for the vehicle and infrastructure.

7.1.1.3 Backend server data loss or compromise

Data held on a backend server might be lost or leaked if it is compromised, by an insider's abuse of authority, unauthorized access from outside or unauthorized physical access, as specified in clause 7.1.1.1. In addition, there are additional threats as follows:

– Loss of information in the cloud: Sensitive information, e.g., vehicle identification number (VIN) or driver's personal information, may be leaked and compromised if they are stored in third-party cloud service provider systems.

– Information breach by unintended sharing of data: If a server is located in an unsecured perimeter caused by an administrator's misconfiguration, data may be inadvertently shared or leaked.

7.1.2 Threats to vehicles regarding their communication channels

Vehicle communication includes external communications such as V2V, V2I, V2D and V2P communications and in-vehicle communications such as controller area network (CAN), local interconnect network (LIN), media-oriented systems transport (MOST), and FlexRay. Channels used in these communications may be targets of attacks like spoofing, eavesdropping or message manipulation, among others.

7.1.2.1 Spoofing messages

Spoofing messages by impersonation can occur. In the case of messages used in a V2X communications and global navigation satellite system (GNSS), invalid messages can be received by a vehicle due to an impersonation attack. In addition, if there are many vehicles on a specific road, a Sybil attack can be carried out in order to spoof other vehicles.

NOTE – A Sybil attack occurs, for example, when one vehicle simulates multiple vehicles by using multiple vehicle IDs.

7.1.2.2 Unauthorized manipulation, deletion or other amendments to vehicle-held code or data

If there is a vulnerability or weakness in the vehicle, illegal remote access or malware intrusion attack can be made through the vehicle's communication channels. As a result, the communication channel may enable many security threats as follows:

– code injection, e.g., software binary code that has been tampered with might be injected into the communication stream;

– manipulation of vehicle-held data or code;

– overwriting of vehicle-held data or code;

– erasure or deletion of vehicle-held data or code;

7.1.2.3 Use of untrusted or unreliable messages and session hijacking or replay attacks

Messages from an unreliable or untrusted source can be received through communication channels. Man-in-the-middle attacks and session hijacking are possible through communication channels. For example, an attack against a communication gateway in the vehicle allows an attacker to downgrade the software of an ECU or firmware of the gateway using known vulnerabilities of the software by a replay attack where repeatedly valid data transfers are made by malicious intent.

7.1.2.4 Information disclosure

Information can be readily disclosed through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders. That is, information exchanged over the communication channel can be eavesdropped by malicious interception, interfering radiation and monitoring communications. To this end, the attacker can gain unauthorized access rights to files.

7.1.2.5 Denial of service attacks

An attacker can conduct a denial of service attack via a communication channel by sending a large volume of garbage data to the vehicle information system so that vehicle functions are mostly disrupted. On the other hand, in the cases of platooning or vehicle-to-vehicle communication, the attacker could prevent necessary data from being sent to the other vehicles in the group so that other vehicles lose control because of lack of data from the other vehicles. This is called a "black hole attack".

7.1.2.6 Privileged access by an unprivileged user

By means of illegal accesses through communication channels, an unprivileged user can gain privileged access, such as root access, to the system. This is called "unauthorized privilege escalation" and once this escalation is successful, an attacker can do things that normal users cannot.

7.1.2.7 Viruses embedded in communication media

After finding vulnerabilities in the vehicle system, viruses or malware can be injected into the vehicle system through communication channels. The viruses can become an administrator with privileged access and can conduct any intended attacks in the vehicle. For example, if the virus encrypts any files and information without authorization in the targeted vehicle system, which is called "ransomware", then the vehicle system will lose its function.

7.1.2.8 Messages with malicious content

Messages received by the vehicle (e.g., diagnostic messages or messages from other vehicles) or transmitted within it, may contain malicious content. In the case of IVNs, an attacker can modify the software of ECUs by means of virus injection (see clause 7.1.2.7) and join the vehicle network as a member by using impersonation.

Malicious V2X messages, such as cooperative awareness messages (CAMs) and decentralized environmental notification messages (DENMs), can be received by neighbouring vehicles. The V2X communication is based on broadcasting, therefore, a lot of malicious V2X messages may cause harmful influence on the whole vehicular networks including IVNs in the vehicle itself.

Malicious diagnostic messages can be also received. An attacker can record a diagnostic message and can use it for a replay attack. Furthermore, even the control message of the vehicle can be received via a replay attack.

Proprietary messages are normally sent from an OEM, or component, system or the function supplier. However, malicious proprietary messages to disrupt the vehicle system can also be received from attackers.

7.1.3 Threats to vehicles regarding their update procedures

There are two ways to update vehicle systems, namely, by wired update through an OBD port and portable devices such as a secure digital (SD) card or by a USB flash drive, and wireless update over the air (OTA). The software to be updated can be firmware or configuration data of the vehicle. Most electronic problem and software defects can be updated and solved electronically without physical access, e.g., via OBD tester. Furthermore, OTA (wireless) updates help in shortening the update cycle to minimize attack exposure for known vulnerabilities of the software.

7.1.3.1 Misuse or compromise of update procedures

Regardless of whether the update used is conducted in a local or physical manner or through OTA, the update procedure can include threats using fabricating system update programs or compromised firmware.

The software can be manipulated before the update process, although the update process is left intact. The software provider creates or prepares software for the update and it is delivered to the target systems that require it. Therefore, there can be a serious threat of software manipulation and corruption before it is put into service.

Especially, cryptographic materials, such as keys and certificates, used in the software update procedure can be compromised and consequently cause invalid software updates.

7.1.3.2 Denial of a legitimate update

Denial of service attack against an update server or network to prevent the rollout of critical software updates or unlock of customer-specific features is possible in the software update procedure. It is also possible to deny legitimate updates.

7.1.4 Threats to vehicles regarding unintended human actions

Human actions can unintentionally introduce unrecognized threats. These threats include, by default, unauthorized or inadvertent modification of the software. Incidental errors include configuration breaches, programming errors and data corruption due to mistakes by the user or operator.

7.1.4.1 Misconfiguration of equipment or systems by a legitimate actor

A legitimate user can take actions that unintentionally induce cyberattacks. The setting of the vehicle system may be abnormally changed by a legitimate user during unintentional installation, repair or use. There may also be mistakes in managing or using systems or devices that include software updates.

7.1.4.2 Unwitting facilitation of a cyber-attack by a legitimate actor

A legitimate user (e.g., owner, operator or maintenance engineer) can be an innocent victim and be tricked into taking an action to unintentionally load malicious code (malware) or enable an attack. Furthermore, the legitimate user often does not follow defined security procedures.

7.1.5 Threats to vehicles regarding their external connectivity and connections

For a variety of convenient services, vehicles can be equipped with components to communicate with backend servers and can communicate to everything enabled by road users over a wireless connection. Besides convenience features, there are safety benefits such as the automatic emergency call functionality and those supported by V2X communication. However, the more vehicles connect to external entities for enhancing connectivity, the more threats and vulnerabilities show up, because attack surfaces are expanded, which are led by additional interfaces.

7.1.5.1 Manipulation of the connectivity of vehicle functions

Manipulation of the connectivity of vehicle functions enables a cyberattack. This threat can be considered in the following vehicle elements:

- manipulation of functions designed to remotely operate systems: remote key, immobilizer, and charging pile;
- manipulation of vehicle telematics: e.g., remotely unlock cargo;
- manipulation through an interface with a short-range wireless system or sensors.

7.1.5.2 Hosted third-party software

An infotainment system in modern vehicles connected to the IVN may allow installation of third party applications. The third party applications can be corrupted or have poor software security and be used as methods to attack vehicle systems.

7.1.5.3 Devices connected to external interfaces

The functions of connectivity bring external interfaces and the devices connected to them can be used as a means to attack vehicle systems with the following vulnerable interfaces:

- external interfaces such as USB port: to attack through code injection;
- infected media with the virus: the virus can attack the in-vehicle system via the infected media;
- diagnostic access: diagnostic functions accessed by Bluetooth dongles in OBD ports are used to view the status of vehicles and manipulate vehicle parameters that are included in the vehicle software.

7.2 Potential information related to threats

7.2.1 Potential targets of, or motivations for, an attack

Vehicles may become the target of potential cyberattacks when they are electronically connected to many systems or services in the vehicle ecosystem. Furthermore, attackers often seek financial benefits by making their attack skills known not only to the world, but also to OEM vendors. The attacks may impact vehicle systems as described in clauses 7.2.1.1 to 7.2.1.7.

7.2.1.1 Extraction of vehicle data or code

Sensitive or credential data are targets for extraction because they may contain the following useful information for financial gain:

– copyright or proprietary software of the vehicle;

– the owner's private information, such as personal identity, payment account information, address book information, location information and vehicle electronic ID;

– cryptographic keys, etc.

7.2.1.2 Manipulation of vehicle data or code

By manipulating the vehicle data or code, attackers could impersonate or repudiate the rightful owner's behaviour. The following manipulation methods can be identified:

– illegal/unauthorized changes to a vehicle's electronic ID;

– identity fraud: if a user wants to display another identity when communicating with toll systems and manufacturer backend systems;

– action to circumvent monitoring systems: hacking, tampering with or blocking messages, such as operating data recorder (ODR) tracker data or number of runs;

– data manipulation to falsify vehicle driving data, e.g., mileage, driving speed, driving directions and vehicle's reference time;

– unauthorized changes to system diagnostic data;

– firmware version fraud: the latest firmware having a patch to counter some vulnerability can be replaced by the old version without the patched.

7.2.1.3 Erasure of data or code

Unauthorized deletion or manipulation of the system event logs may occur. This falsification often makes it impossible to analyse data or makes it difficult to search for the cause of the attack.

7.2.1.4 Introduction of malware

By using many attack methods, introducing malware into a vehicle system is the first step in an attacker's activity. There are various attack interfaces for introducing malware, such as using external interfaces and infected physical modules.

7.2.1.5 Introduction of new software or overwriting existing software

The introduction of new software or the overwriting of existing software with that which is malicious, may have a serious cybersecurity impact on the vehicle control system or information system.

7.2.1.6 Disruption of systems or operations

A denial of service attack against the vehicle system may be triggered on the internal network by flooding messages in a CAN bus or by provoking faults on an ECU via a high rate of messages.

7.2.1.7 Manipulation of vehicle parameters

Manipulation of vehicle parameters may have a strong influence on the vehicle system, e.g., unauthorized access to falsify:

– the configuration parameters of a vehicle's key functions, such as brake data or airbag deployment threshold;

– the charging parameters, such as charging voltage, charging power, battery temperature, etc.

7.2.2 Potential vulnerabilities

7.2.2.1 Vulnerable cryptographic technologies

Cryptographic technologies can be compromised or are insufficiently applied. Cryptographic keys or certificates including credentials, such as password, can be exploited. For example, if weak cryptographic keys are used or the cryptographic keys are not updated for a long time, the cryptographic system may be broken by brute force attacks. Insufficient use of cryptographic technologies can also lead to leakage of cryptographic keys or credentials. Furthermore, the risk of information leakage can be increased by the use of already broken and obsolete cryptographic technologies.

7.2.2.2 Compromised vehicle parts or supplies

Hardware or software used in a vehicle ecosystem can be engineered so that it fails to meet design criteria to defend against an attack. Parts or supplies in a vehicle can be compromised to permit vehicles to be attacked.

7.2.2.3 Vulnerabilities in software or hardware development

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

Using remainders from development (e.g., debug ports, joint test action group (JTAG) ports, microprocessors, development certificates and developer passwords) can also permit access to ECUs or permit attackers to gain higher privileges.

7.2.2.4 Vulnerabilities in network design

If network access is allowed while unnecessary communication ports are left open, attacks such as unauthorized access are likely to increase.

Furthermore, the use of unprotected gateways or access points (such as truck-trailer gateways) to circumvent protections and gain access to other network segments, can result in the performance of malicious acts, such as sending arbitrary CAN bus messages.

7.2.2.5 Physical loss of data

Sensitive data used in vehicle ecosystems can be lost or compromised due to physical damage because of traffic accidents or theft. Data loss from digital rights management (DRM) can also occur, such as deletion of user data.

Furthermore, the integrity of sensitive data may be lost due to wear and tear on information technology (IT) components, causing potential cascading issues (e.g., in the case of key alteration).

7.2.2.6 Unintended transfer of data

Private or sensitive data can be leaked when the users of a vehicle change (e.g., when the vehicle is sold or used for hire with a different person).

7.2.2.7 Physical manipulation of systems

Physical manipulation of systems such as OEM hardware is likely to lead to attacks. For example, a man-in-the-middle attack is possible if unauthorized hardware is added to the vehicle.

Appendix I

Examples of vulnerability or attack method related to threats

(This appendix does not form an integral part of this Recommendation.)

This appendix provides examples of vulnerability or attack methods related to threats reproduced from Table 1 of [b-UNECE GRVA].

NOTE – The clause numbers in the leftmost column of Table I.1 are those used in [b-UNECE GRVA].

Table I.1 – List of examples of vulnerability or attack methods related to threats

High level and sub-level descriptions of vulnerability/threat			Example of vulnerability or attack method	
4.3.1 Threats regarding back-end servers	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (insider attack)
			1.2	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on
	3	Data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (insider attack)
			3.2	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
			3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	Unauthorised physical access to the server (conducted for example by USB sticks or other media connecting to the server)
			3.5	Information breach by unintended sharing of data (e.g., admin errors, storing data in servers in garages)
4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	Spoofing of messages by impersonation (e.g., 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
	5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit manipulate of vehicle held data/code
			5.3	Communications channels permit overwrite of vehicle held data/code
			5.4	Communications channels permit erasure of vehicle held data/code
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)
	6	Communication channels permit untrusted/unreliable messages to be accepted or are	6.1	Accepting information from an unreliable or untrusted source
			6.2	Man in the middle attack/ session hijacking

Table I.1 – List of examples of vulnerability or attack methods related to threats

High level and sub-level descriptions of vulnerability/threat			Example of vulnerability or attack method	
		vulnerable to session hijacking/replay attacks	6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway
	7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	Interception of information/interfering radiations/ monitoring communications
			7.2	Gaining unauthorised access to files or data
	8	Denial of service attacks via communication channels to disrupt vehicle functions	8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner
			8.2	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
	9	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to gain privileged access, for example root access
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	Virus embedded in communication media infects vehicle systems
	11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious internal (e.g., CAN) messages
			11.2	Malicious V2X messages, e.g., infrastructure to vehicle or vehicle-vehicle messages (e.g., CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious proprietary messages (e.g., those normally sent from OEM or component/system/function supplier)
4.3.3. Threats to vehicles regarding their update procedures	12	Misuse or compromise of update procedures	12.1	Compromise of over the air software update procedures. This includes fabricating system update program or firmware
			12.2	Compromise of local/physical software update procedures. This includes fabricating system update program or firmware
			12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact
			12.4	Compromise of cryptographic keys of the software provider to allow invalid update
	13	It is possible to deny legitimate updates	13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features
4.3.4 Threats to vehicles regarding unintended human actions	14	Misconfiguration of equipment or systems by legitimate actor, e.g., owner or maintenance community	14.1	Misconfiguration of equipment by maintenance community or owner during installation/repair/use causing unintended consequence
			14.2	Erroneous use or administration of devices and systems (incl. OTA updates)
	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1	Innocent victim (e.g., owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack
			15.2	Defined security procedures are not followed

Table I.1 – List of examples of vulnerability or attack methods related to threats

High level and sub-level descriptions of vulnerability/threat			Example of vulnerability or attack method	
4.3.5 Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of functions designed to remotely operate systems, such as remote key, immobiliser, and charging pile
			16.2	Manipulation of vehicle telematics (e.g., manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
			16.3	Interference with short range wireless systems or sensors
	17	Hosted 3rd party software, e.g., entertainment applications, used as a means to attack vehicle systems	17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems
	18	Devices connected to external interfaces e.g., USB ports, OBD port, used as a means to attack vehicle systems	18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a virus connected to a vehicle system
			18.3	Diagnostic access (e.g., dongles in OBD port) used to facilitate an attack, e.g., manipulate vehicle parameters (directly or indirectly)
4.3.6 Potential targets of, or motivations for, an attack	19	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy)
			19.2	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.
			19.3	Extraction of cryptographic keys
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorised changes to vehicle's electronic ID
			20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
			20.3	Action to circumvent monitoring systems (e.g., hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4	Data manipulation to falsify vehicle's driving data (e.g., mileage, driving speed, driving directions, etc.)
			20.5	Unauthorised changes to system diagnostic data
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of system event logs
	22	Introduction of malware	22.2	Introduce malicious software or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1	Fabrication of software of the vehicle control system or information system
	24	Disruption of systems or operations	24.1	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
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of falsify the configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.

Table I.1 – List of examples of vulnerability or attack methods related to threats

High level and sub-level descriptions of vulnerability/threat			Example of vulnerability or attack method	
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated cryptographic algorithms
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack
	28	Software or hardware development permits vulnerabilities	28.1	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.
			28.2	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
	29	Network design introduces vulnerabilities	29.1	Superfluous internet ports left open, providing access to network systems
			29.2	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
	30	Physical loss of data can occur	30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft
			30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues
			30.3	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)
	31	Unintended transfer of data can occur	31.1	Information breach. 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)
	32	Physical manipulation of systems can enable an attack	32.1	Manipulation of OEM hardware, e.g., unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ISO/IEC 27000] ISO/IEC 27000:(2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-UNECE GRVA] UNECE GRVA-01-17 (2017), *Draft Recommendation on cyber security of the Task Force on Cyber Security and Over-the-air* Issues *of UNECE WP.29 GRVA*. Available [viewed 2020-08-07] at: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020