ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1382 (03/2023)

SERIES X: Data networks, open system communications and security

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

Guidelines for sharing security threat information on connected vehicles

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1399**
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1382

Guidelines for sharing security threat information on connected vehicles

Summary

Connected vehicles are facing increasingly prominent network security issues along with their rapid development. Security threat information of connected vehicles, which plays an integral role in securing connected vehicles, is any information that can help an organization identify, assess, monitor, and respond to a connected vehicle. Organizations that share threat information for connected vehicles can improve their own security postures and those of other organizations.

Recommendation ITU-T X.1382 provides guidance on the principles, rules, methodology and procedures of sharing security information for connected vehicles. It also provides a brief description of the different scopes, roles and effectiveness of the various organizations while they engage in the lifecycle of security threat information sharing.

This Recommendation is intended to help organizations stay in touch with the connected vehicles sharing community and to contribute threat information which would support the practices of connected vehicles safety protection. Overall, this Recommendation aims to enhance security threat information sharing and mitigate the potential impact of cybersecurity attacks on connected vehicles.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1382	2023-03-03	17	11.1002/1000/15104

Keywords

Connected vehicles, threat information sharing.

[*] 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1382

Guidelines for sharing security threat information on connected vehicles

1 Scope

The purpose of this Recommendation is to provide guidelines for sharing threat information of connected vehicles ecosystems, including the roles and partnership of organizations, sharing scopes, procedures and requirements for sharing threat information of connected vehicles.

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.

[ITU-T X.1371] Recommendation ITU-T X.1371 (2020), *Security threats to connected vehicles.*

[NIST SP 800-150] *Guide to Cyber Threat Information Sharing.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 alert [NIST SP 800-150]: A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.

3.1.2 security threat information [NIST SP 800-150]: Information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.

3.1.3 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

This Recommendation defines the following terms:

3.2.1 actor tactics: Descriptions of the technical goals of an actor to perform an action.

3.2.2 actor techniques: Descriptions of how an actor achieves the technical goals by performing an action.

3.2.3 actor procedures: Descriptions of an actor's implementation of specific technique.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
APP	Application

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ECU	Electronic Control Unit
GSMA	GSM Association
ISAC	Information Sharing and Analysis Centre
MEC	Multi-access Edge Computing
T-BOX	Telematics BOX
TSP	Telematics Service Provider
TTP	Tactics, Techniques and Procedures
V2X	Vehicle-to- Everything

5 Conventions

In this Recommendation:

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview

The main elements of threat information sharing on connected vehicles include types of threat information, sharing principles, roles, rules, communities and procedures. In general, different organizations on connected vehicles generate different types of security threat information. Different types of agents play different roles in the threat information sharing activities on connected vehicles. The threat information sharing activities on connected vehicles among organizations need to follow certain principles, rules and procedures, while threat information has different effects. Different organizations can form a sharing community according to a certain sharing mode and a sharing platform.

6.1 Types of threat information on connected vehicles

Referring to [NIST SP 800-150], threat information on connected vehicles can be classified as indicators, tactics, techniques and procedures (TTPs), security alerts, and threat intelligence reports:

a) Indicators are observable signs that an attack is imminent or in progress. Indicators can be used to detect and act against potential threats. Some indicators of connected vehicles include organizations of suspected vehicle-to-everything (V2X) attackers.

b) TTPs describe the behaviour of an actor. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism, or exploitation system. There are a variety of threats including threats regarding back-end servers and the server, and threats to vehicles regarding their communication channels. TTP may include actions to manipulate the connectivity of vehicle functions or to circumvent the monitoring system, which are different from traditional network threats.

c) Security alerts are technical notifications about vulnerabilities, exploits, malware and other security issues. Security alerts usually originate from reputable sources such as computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs). Security alerts are issued when the affected connected vehicles are diverse or when threats could cause huge harm.

d) Threat intelligence reports provide deep analysis on threats including the event participants, target system, attack type and other information, and provide advice on actions to mitigate threats. Threat intelligence reports can also show the future trends of threats. Threat intelligence reports play an important role in preventing the occurrence of new attacks on connected vehicles.

6.2 Benefits and challenges of sharing threat information on connected vehicles

Using shared threat information on connected vehicles, organizations related to the connected vehicles industry can enhance their security posture by leveraging their partners' knowledge, experience, and capabilities in a proactive way. Benefits of sharing threat information on connected vehicles include:

a) Enhancing the defence capability of organizations on connected vehicles. Connected vehicles involve new threats, while information sharing can help organizations improve their threat defence capabilities. New vulnerabilities are often used as the primary tool for attacks. Threat information sharing can deal with new vulnerability attacks in time, and improve the ability of attack defence. While connected vehicles face many new attacks, threat information sharing helps deal with new threats on connected vehicles and improves defence capability.

b) Keeping the connected vehicles ecosystem healthy. Threat information sharing helps to promote the security of connected vehicles economic environment and to establish the ecological security of all connected vehicles. The security of connected vehicles manufacturing chain includes the security of service providers, telematics service provider (TSP), vehicle manufacturing enterprises, telecommunication operators, vehicle and handheld terminal equipment providers, mobile intelligent terminal equipment providers, etc.

While sharing threat information has benefits, certain challenges remain. Challenges of information sharing include:

a) Establishing threat information of a connected vehicles sharing standard system. In order to keep the connected vehicles ecosystem healthy, it is necessary to formulate a reasonable standard system for sharing threat information of connected vehicles. At present, there is no unified international standard system for sharing threat information of connected vehicles. If the standard system is not established, it will hinder the information sharing and ultimately affect its development.

   NOTE – Some guidelines such as [ITU-T X.1371] and GSMA IoT security guidelines [b-GSMA CLP.11] can provide the security issues to be considered as possible best practices for information sharing.

b) Defining threat information scope. The connected vehicles industrial chain is composed of different links, and each link faces different types of threats. It is necessary to define the threat information sharing in each link and the information sharing mode between links.

c) Protecting sensitive and classified information. Sharing threat information of connected vehicles faces the risk of sensitive information disclosure. Cryptographic technologies can be compromised or are insufficiently applied. 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 using already broken and obsolete cryptographic technologies. Sensitive information to be protected includes 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 identifier; cryptographic keys and so on. In addition, unauthorized organizations are not permitted access to classified information. Acquiring and maintaining the clearances needed for ongoing access to classified information sources is expensive and time-consuming for organizations.

7 Principles of sharing threat information on connected vehicles

To ensure the effectiveness, accuracy and security of the sharing and transmission process of threat information sharing, it is necessary that organizations and enterprises follow some principles.

7.1 Mutual benefit

The essence of security threat information sharing is to enhance the protection capability of network security on connected vehicles through collaborative efforts. The participating parties of security threat information sharing on connected vehicles are recommended to be aware of the mutual rights, duties and liabilities in the threat information sharing activities. Besides receiving threat information related to their own organization, the organization is also recommended to actively contribute its own efforts to achieve mutual benefits and win-win situations.

7.2 Categorization and classification

Different organizations play different roles in the security threat information sharing process. Given certain threat information, the meaning and importance for different organizations appear to be diverse. Organization is recommended to categorize and classify threat information on connected vehicles, and define the effective scope. Different levels of the management system are recommended to be established according to their categorization, classification and scope tags. Appropriate cryptography is recommended to be used to keep the sensitive information's confidentiality and integrity and/or authenticity protection.

7.3 Data security

Problems such as illegal use, theft and tampering of threat information data and unauthorized access by users seriously affect data sharing parties' initiative to intelligence sharing and reduce the security and effectiveness of intelligence sharing activities. For this reason, the control of sharing risk is also the focus of threat information sharing. Countermeasures including the cryptography, desensitization of shared data, identification and destruction, etc., are effective in protecting data related to threat information on connected vehicles security.

8 Organization, role and partnership

8.1 Organizations and their roles

8.1.1 Automakers

Automakers play the most important role in threat information sharing activities on connected vehicles because automakers directly interact with users and they are responsible for the security of their vehicles.

Through collecting data from their own production systems, on-board components, and connected vehicle infrastructure, automakers collect, integrate, produce and analyse security threat information related with connected vehicles, and take measures to mitigate threats.

8.1.2 Suppliers

Suppliers provide in-vehicle hardware or software for connected vehicles, including vehicle chips, telematics BOX (T-BOX) equipment and internal/external gateways. Suppliers collect and receive security threat information related to their products, and assist the coordination team, automobile manufacturers and other relevant parties to mitigate threats and/or prevent and reduce security incidents related to their products.

8.1.3 Third party product and service providers

Third party product and service providers mainly refer to organizations that provide independent products and services related to the connected vehicles besides automobile manufacturers and their parts suppliers, such as TSP, cloud computing service providers, hardware vendors, mobile terminal manufacturers, vehicle insurance service providers, other third-party service platform operators, etc.

Third party product and service providers collect/produce/share information of security threats on their products or service platforms, such as threat information on failure of connected vehicles, unauthorized user behaviour, or remote attacks, and assist relevant parties such as coordination teams for connected vehicles and automobile manufacturers in mitigating threats and/or dealing with security incidents in connected vehicles. Cloud computing service providers are also responsible for sharing information including misconfiguration or errors, abuse of control ports, improper credentials management, cloud data leakage, etc.

8.1.4 Coordination team

The coordination teams for connected vehicles usually work as independent entities which focus on the coordination of security threat information and incident response, such as CERTs/CSIRTs, and Auto-ISAC.

Coordination teams for connected vehicles assist relevant parties in cross-organizational coordination of information sharing on security threats, and provide notification and early warning services for relevant parties.

8.1.5 Telecommunication operators

Telecommunication operators provide basic telecommunication services for connected vehicles.

Telecommunication operators ensure the security of the telecommunication network infrastructure such as core networks, base stations, MEC platforms, etc.

NOTE – As an example of telecommunication operators in the context of connected vehicle, GSMA guidelines for network operators [b-GSMA CLP.14] can be considered.

8.1.6 Cybersecurity vendors

Cybersecurity vendors are network-related companies or organizations involved in vehicle enterprises and organizations that provide cybersecurity products or services.

Through sources such as security devices, terminal software and Internet, cybersecurity vendors assist relevant organizations in collecting, integrating and analysing security threat information on connected vehicles, and provide security support and services to prevent and reduce security incidents.

8.2 Sharing scopes among organizations

Organizations are recommended to define the scope of information sharing activities, including identifying the types of threat information which can be shared, the circumstances under which threat information sharing activities are permitted, and the sharing priority of threat information on connected vehicles.

The breadth of information sharing activities will vary based on an organization's resources and abilities. The scopes of sharing threat information on connected vehicles vary among different types of organizations. For example, the scopes are diverse among cybersecurity vendors, automakers, V2X equipment providers, communication equipment providers and telecommunication operators, etc. The producers of threat information concerning connected vehicles with limited resources are recommended to focus on a smaller set of threat producing/collecting activities that provide threat information with higher value to the organization and their sharing partners. An organization may be able to expand the scope of sharing threat information as additional capabilities and resources. An organization with greater resources and advanced capabilities may choose a larger initial scope that allows for a broader set of threat information sharing activities to support their goals and objectives.

Table 1 introduces which organizations can be influenced by each type of threat defined in [ITU-T X.1371].

Table 1 – Mapping of different organizations influenced by each threat type on connected vehicles

Type of threats	**Organizations to share threat information**					
	Automakers	**Suppliers**	**Third party product and service providers**	**Coordination team**	**Telecommunication operators**	**Cybersecurity vendors**
Threats regarding back-end servers	✓		✓	✓		✓
Threats to vehicles regarding their communication channels	✓	✓	✓	✓	✓	✓
Threats to vehicles regarding their update procedures	✓		✓	✓		✓
Threats to vehicles regarding unintended human actions	✓	✓	✓			
Threats to vehicles regarding their external connectivity and connections	✓	✓	✓	✓	✓	✓
Potential targets of, or motivations for, an attack	✓	✓	✓	✓		✓
Potential vulnerabilities	✓	✓	✓	✓	✓	✓

8.3 Information sharing rules among organizations

Based on the characteristics and classification of threat information on connected vehicles, rules of threat information sharing among organizations can be described as follows:

a) Organizations are recommended to share threat information on connected vehicles.

b) Sharing of threat information of connected vehicles often occurs at connected vehicles management platforms, shared travel service providers, vehicle manufacturing enterprises, V2X equipment providers, communication equipment providers and telecommunication operators.

c) Many organizations such as automakers and cybersecurity vendors play a role both as threat information producers and consumers.

d) Threat information producers are recommended to be professional.

e) Management requirements such as threat information filtering and subscription verification are recommended.

8.4 Establishing a sharing community

A community is recommended to be established to share and analyse threat information on connected vehicles. Threat information sharing models include peer-to-peer, source and subscriber and hub and spoke [b-OASIS TAXII]. Through a sharing community, organizations can receive real-time network threat and vulnerability data on connected vehicles. Auto-ISAC, which was established by automobile enterprises in 2015, is an example. It focuses on setting up an information sharing community with an increasing number of intelligent vehicles. Auto-ISAC's portal allows its members to submit and receive information anonymously, and helps members deal with network threats more effectively. Auto-ISAC has been actively promoting cooperation and information sharing among suppliers, commercial vehicle companies and automobile manufacturers in the field of vehicle network security. Appendix I provides an introduction to Auto-ISAC's threat information sharing activities.

A sharing community can set up multiple sharing sub-communities, and organizations can choose to join one or more sub-communities related to connected vehicles. The sharing community is recommended to be an open community, which allows different organizations to join and exit freely through voluntary cooperation. When choosing to join the sub-community, the organization is recommended to choose the community with complementary threat information resources on connected vehicles. Each organization voluntarily publishes the threat information of connected vehicles to the sharing community, and is responsible for ensuring that the threat information provided to the community is suitable for sharing.

9 Procedures and guidance for sharing threat information on connected vehicles

9.1 Introduction

[ITU-T X.1371] defines and describes threats of connected vehicles. Organizations can detect, analyse and handle security threats with internal resources, and can also share threat information by establishing a cross-organizational sharing framework. In a cross-organizational sharing procedure, organizations can:

a) Acquire and use external threat information to prevent and mitigate threats on connected vehicles.

b) Produce and provide threat information on connected vehicles with other organizations to enhance vehicles' ecosystem security.

According to the threat information transmission chain posture, organizations can be sorted into two types, consumers and producers. Many organizations such as automakers and cybersecurity vendors usually play roles both as threat information producers and threat information consumers.

9.2 Procedures of threat information sharing activities

Consumers are the potential victim of the threat of connected vehicles. By acquiring and using threat information, consumers can quickly locate the impacted assets and take necessary countermeasures to mitigate threats. Among all relevant organizations, automakers are the core threat information consumers. The procedures for consumers consist of five phases:

a) Preparation: Developing appropriate mechanisms to get ready for the engagement of threat information sharing activities;

b) Receipt: Receiving external threat information;

c) Analysis: Performing analysis for the received threat information;

d) Mitigation: Taking measures to mitigate threats based on the analysis results;

e) Prevention: Actions to prevent future occurrences.

Producers are entities with technical capacity, analytical ability and sharing intention in a vehicle ecosystem. Normally, producers also need to consume security threat information because producing/collecting threat information needs multiple sources, among which are the received threat information. The procedures for producers consist of three phases:

a) Preparation: Developing appropriate mechanisms to get ready for the engagement of threat information sharing activities;

b) Analysis: Performing analysis to produce high quality threat information;

c) Sharing: Sharing the produced threat information to interested parties.

9.3 Guidance during phases in the procedures

9.3.1 Guidance for organizations as consumers

9.3.1.1 Guidance in the preparation phase

Organizations are recommended to develop their policy on security threat information for connected vehicles, including setting the goal, defining the scope, and establishing the decision-making process. The guidance are as follows:

a) Setting the goal: Organizations need to take note that they are facing security threats. Based on the analysis of the organizations' security threats, organizations are recommended to establish their safety objectives to enhance their safety protection capability.

b) Defining the scope: Combining with the organizations' security objectives, technical capabilities, financial budget and the potential impact of various threats to the organization, the scope of threat information needed by the organization is recommended to be defined and the priority is recommended to be determined.

c) Establishing decision-making process: The time required for decision-making is recommended to be determined according to the type and priority of threat information needed by the organization, so as to avoid the impact of a long decision-making process on the timely disposal of threat information.

9.3.1.2 Guidance in the receipt phase

The guidance is as follows:

a) Organizations are recommended to properly store the shared security threat information.

b) Organizations are recommended to take measures to ensure the security of threat information storage.

c) Organizations are recommended to erase obsolete and useless threat information.

9.3.1.3 Guidance in the analysis phase

The guidance is as follows:

a) Organizations are recommended to evaluate the value of threat information. Appendix II shows a reference methodology to evaluate the value of threat information. Automatic evaluation is recommended.

b) Organizations are recommended to verify and carry out analysis to assess the potential damage to their products and services.

c) Organizations are recommended to analyse context to identify information such as attackers, TTP, and targets.

d) Organizations are recommended to identify the affected assets, such as servers, domain(s), electronic control units (ECUs), system(s), etc.

e) Organizations are recommended to filter, verify and carry out analysis in a secure environment to avoid the impact on critical systems of organizations.

9.3.1.4 Guidance in the mitigation phase

The guidance are as follows:

a) Organizations are recommended to develop handling solutions and implement their handling processes based on the threat information and the analysis results. Solutions include isolating affected hardware, implementing patches, updating software, modifying configuration, etc.

b) If organizations lack handling capacity, organizations are recommended to contact coordination teams for connected vehicles and seek assistance.

c) For indicators, organizations are recommended to deploy received indicators to cybersecurity devices.

d) For the security threats brought by legitimated users through modification of configuration and dissemination of malicious programs, organizations are recommended to immediately analyse and strengthen management. Organizations can repair and manage the exploitable vulnerabilities, defects or improper configuration in the network by using threat information including disposal measures.

9.3.1.5 Guidance in the prevention phase

Organizations are recommended to continue monitoring their products and services.

9.3.2 Guidance for organizations as producers

9.3.2.1 Guidance in the preparation phase

Organizations are recommended to develop their policy, including setting the goal, defining the scope, and establishing the decision-making process. The guidance is as follows:

a) Organizations are recommended to establish a response management process to prevent the leakage of important data.

b) Organizations are recommended to deploy essential resources and tools for generating indicators and other threat data.

c) Organizations are recommended to identify, evaluate and classify the multi-source heterogeneous network threat data, so as to ensure that all the information related to the threat is fully described and updated at any time.

d) Organizations are recommended to set up or join in a sharing community, obtain data by purchasing/receiving non-public intelligence and collecting public intelligence, analyse these data according to some application scenarios and business requirements, and then produce the corresponding threat intelligence. In the framework of sharing, a sharing community integrates the threat information shared by all members according to the actual needs to produce more targeted, more complete and accurate threat intelligence, and shares it in the form of open source or paid sales according to the type and value of intelligence.

e) Organizations are recommended to define the scope of information sharing activities, including defining threat information to be shared, deciding the exchange format.

9.3.2.2 Guidance in the analysis phase

The guidance is as follows:

a) Organizations are recommended to filter the alarm logs automatically or manually to remove worthless alarms or even false alarms.

b) Organizations are recommended to assess the value of shared information and determine the scope of the sharing organization.

c) Organizations are recommended to define the observability of different network threat scenarios and their related metadata, and then analyse and process the comparison results of these threat characteristic indicators.

9.3.2.3 Guidance in the sharing phase

The guidance is as follows:

a) Organizations are recommended to implement threat information sharing following the defined scope.

b) Organizations are recommended to provide security threat information in standardized format.

c) Organizations are recommended to provide more contextual information.

d) Organizations are recommended to formulate the sharing model and mechanisms, and solve the intelligence exchange sharing validity and the transaction fairness questions.

e) With the development needs of the industry, it is recommended to establish a connected vehicles threat information sharing exchange platform to carry out information sharing.

f) Organizations are recommended to establish a control mechanism for threat information data sharing, including desensitization, authentication and destruction of shared data.

g) With the ability to produce threat information on connected vehicles, organizations are recommended to share threat information with organizations of good reputation.

Appendix I

Best practice for Auto-ISAC's threat information sharing activities

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

The Automotive Information Sharing and Analysis Center [b-AUTO-ISAC] released a best practice guide *"Collaboration and engagement with appropriate third parties"* version 1.3 in 2019. In this best practice guide, Auto-ISAC provides best practice for information sharing which includes relevant third parties, level of openness, content that is helpful to share, and information sharing processes, etc.

To enhance vehicle cybersecurity, these organizations may collaborate and engage with several types of third parties across the connected vehicle ecosystem. Relevant third parties include industry partners, industry organizations, government, academia, researchers and media.

Organizations can determine the right level of openness based on their individual vehicle cybersecurity objectives and their unique risk landscape. Level of openness can be divided into limited, moderate and extensive.

The key processes to share information among different stakeholders include:

a) Identifying content that is helpful to share.

b) Engaging the right internal stakeholders.

c) Creating processes to take in and act on shared information.

d) Creating processes to push information to external third parties.

e) Acquiring appropriate tools and technologies.

Appendix II

Methodology for evaluating the value of threat information

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

When evaluating the value of each threat information, organizations can evaluate from five factors as listed below:

a) Reputation of threat sources: Reputation of threat sources are different. Sources which have high confidence can provide more valuable threat information.

b) Timeliness: Threat information is time-sensitive. Earlier information can help organizations to protect and prevent attacks on its assets.

c) Completion of the description: Normally, threat information with more detailed description and contextual information are more valuable.

d) Relevance and impact to the organization: Some threat information targets a specific industry, specific products or even specific companies. Threat information related to the organization needs to be specially noticed.

e) Effectiveness of threat information: Multiple resources cause duplication and collisions of threat information, merging of the similar threats and determination of the authenticity can improve the efficiency of threat information in an organization.

Bibliography

[b-AUTO-ISAC] *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide, Version 1.3, 2019.*

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

[b-GSMA CLP.11] GSMA CLP.11 (2020), *IoT Security Guidelines Overview Document, Version 2.2.*

[b-GSMA CLP.14] GSMA CLP.14 (2020), *IoT Security Guidelines for Network Operators, Version 2.2.*

[b-OASIS TAXII] *OASIS Committee Specification, TAXII™ Version 2.1.*

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

Published in Switzerland
Geneva, 2023