ETSI TR 102 893 V1.2.1 (2017-03)

Intelligent Transport Systems (ITS);
Security;
Threat, Vulnerability and Risk Analysis (TVRA)

Reference

RTR/ITS-0050018

Keywords

authentication, authorization, confidentiality, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.3] operating in a fully deployed ITS.

The present document was prepared using the TVRA method described in ETSI TS 102 165-1 [i.1].

NOTE: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the ETSI ITS Work Programme.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] ETSI TS 102 731: "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

[i.3] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

[i.4] IEEE 802.11TM: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.5] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.6] IETF RFC 4120: "The Kerberos Network Authentication Service (V5)".

NOTE: Available at http://tools.ietf.org/html/rfc4120.

[i.7] ETSI TS 102 636-4-1: "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.9] ETSI TR 102 863: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization".

[i.10] ETSI EN 302 636-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality".

[i.11] Risk analysis study of ITS communication architecture, R Moalla, H Labiod, B Lonc, N Simoni, IEEE Network of the Future conference, 2012.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

beaconing: network layer service which retransmits requested information

end user: functional agent directly representing the human user of the ITS or the ITS service provider

geo-addressing: network layer service that enables the addressing a specific geographic region

ITS application: entity that defines and implements an ITS use case or a set of ITS use cases

ITS use case: specific scenario in which ITS messages are exchanged

ITS user: any ITS application or functional agent sending, receiving or accessing ITS-related information

local dynamic map: dynamically maintained information on driving and environmental conditions in the vicinity of the ITS-S

restricted local ITS station data: data to be shared only with authorized parties

unrestricted local ITS station data: data that may be shared without requiring authorization from the recipient

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Attribute Authority
AC	Attribute Certificate
BSA	Basic Set of Applications
CA	Co-operative Awareness
CAM	Cooperative Awareness Message
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CN	Co-operative Navigation
CS	Communities Services
CSM	Co-operative Speed Management
DENM	Decentralized Environmental Notification Message
DNM	Decentralized environmental Notification Message
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
FA	Functional Asset
FM	Frequency Modulation
GAC	GeoAnycast
GBC	GeoBroadcast
GNSS	Global Navigation Satellite System
GUC	GeoUnicast
HMAC	Hashed Message Authentication Code

HMI	Human-Machine Interface
I2V	Infrastructure to Vehicle
IAAA	Identification, Authentication, Authorization, Accountability
INS	Inertial Navigation System
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	ITS Station
LBS	Location Based Services
LCM	Life Cycle Management
LDM	Local Dynamic Map
OS	Operating System
PKI	Public Keying Infrastructure
PMI	Privilege Management Infrastructure
RHW	Road Hazard Warning
RSU	Road Side Unit
SAML	Security Assertion Markup Language
SFR	Security Functional Requirement
SHB	Single-Hop Broadcast
SoA	Source of Authority
SSP	Service Specific Permissions
ToE	Target of Evaluation
TSB	Topologically-Scoped Broadcast
TTP	Trusted Third Party
TVRA	Threat, Vulnerability and Risk Analysis
UTC	Universal Coordinated Time
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VIN	Vehicle Identification Number

4 The TVRA Method

Without an understanding of the threats posed to a system it is impossible to select or devise appropriate measures to counter these threats. The ETSI Threat, Vulnerability and Risk Analysis (TVRA) [i.1] is used to identify risks to a system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system.

The TVRA method process consists of the following steps:

1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

10) Specification of detailed requirements for the security services and capabilities from step 9.

The present document summarizes the results from each of these steps in the analysis of the ETSI Intelligent Transport System (ITS) standards.

5 The ETSI Intelligent Transport System

5.1 ITS architecture

5.1.1 General

The ITS security architecture is defined in ETSI TS 102 940 [i.8] and covers both the Communication Architecture and the architecture of the ITS-S itself. ETSI TR 102 638 [i.3] defines the basic set of ITS applications which it divides into groups according to the functionality provided which is further analysed in ETSI TR 102 863 [i.9] and transformed into a detail classification of ITS applications in ETSI TS 102 940 [i.8]. For ease of reading and for further risk analysis the relevant tables from ETSI TS 102 940 [i.8] are copied here.

Table 1: ITS application classes

Applications Class	Application	Use case
Active road safety	Driving assistance - Co-operative Awareness (CA)	Emergency vehicle warning
		Slow vehicle indication
		Across traffic turn collision risk warning
		Merging Traffic Turn Collision Risk Warning
		Co-operative merging assistance
		Intersection collision warning
		Co-operative forward collision warning
		Lane Change Manoeuvre
	Driving assistance - Road Hazard Warning (RHW)	Emergency electronic brake lights
		Wrong way driving warning (infrastructure based)
		Stationary vehicle - accident
		Stationary vehicle - vehicle problem
		Traffic condition warning
		Signal violation warning
		Roadwork warning
		Decentralized floating car data - Hazardous location
		Decentralized floating car data - Precipitations
		Decentralized floating car data - Road adhesion
		Decentralized floating car data - Visibility
		Decentralized floating car data - Wind
		Vulnerable road user Warning
		Pre-crash sensing warning
		Co-operative glare reduction
Cooperative traffic efficiency	Co-operative Speed Management (CSM)	Regulatory/contextual speed limits notification
		Curve Warning
		Traffic light optimal speed advisory
	Co-operative Navigation (CN)	Traffic information and recommended itinerary
		Public transport information
		In-vehicle signage

Applications Class	Application	Use case
Co-operative local services	Location Based Services (LBS)	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities Services (CS)	Insurance and financial services
		Fleet management
		Loading zone management
		Theft related services/After theft vehicle recovery
	ITS station Life Cycle Management (LCM)	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration
	Transport related electronic financial transactions (road tolls)	

5.1.2 Summary of ITS applications

In order to define security classes the communication patterns of the different applications also need to be considered. Table 2 summarizes the communication behavior of each application.

Table 2: ITS applications communication behavior

Use case		Addressing	Hops	Frequency	Direction	Session
Emergency vehicle warning		Broadcast	Single	High	V2V/V2I	No
Slow vehicle indication		Broadcast	Single	High	V2V	No
Across traffic turn collision risk warning		Broadcast	Single	High	V2V	No
Merging Traffic Turn Collision Risk Warning		Broadcast	Single	High	V2V/I2V	No
Co-operative merging assistance		Broadcast	Single	High	V2V/I2V	No
Intersection collision warning		Broadcast	Single	High	V2V/I2V	No
Co-operative forward collision warning		Broadcast	Single	High	V2V	No
Lane Change Manoeuvre		Broadcast	Single	High	V2V	No
Emergency electronic brake lights		Broadcast	Multi	Low	V2V	No
Wrong way driving warning (infrastructure based)		Broadcast	Single	Low	I2V	No
Stationary vehicle - accident		Broadcast	Multi	Low	V2V/V2I	No
Stationary vehicle - vehicle problem		Broadcast	Multi	Low	V2V/V2I	No
Traffic condition warning		Broadcast	Multi	Low	V2V/I2V	No
Signal violation warning		Broadcast	Single	High	I2V	No
Roadwork warning		Broadcast	Multi	Low	I2V	No
Decentralized floating car data - Hazardous location		Broadcast	Multi	Low	V2V/I2V	No
Decentralized floating car data - Precipitations		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Road adhesion		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Visibility		Broadcast	Multi	Low	V2V	No
Decentralized floating car data - Wind		Broadcast	Multi	Low	V2V	No
Vulnerable road user Warning		Broadcast	Single	Low	V2V/I2V	No
Pre-crash sensing warning	Indication	Broadcast	Single	High	V2V	No
	Data exchange	Unicast	Single	High	V2V	Yes
Co-operative glare reduction		Broadcast	Single	Low	V2V/I2V	No
Regulatory/contextual speed limits notification		Broadcast	Single	Low	I2V	No
Curve Warning		Broadcast	Single	Medium	I2V	No
Traffic light optimal speed advisory		Broadcast	Multi	Medium	I2V	No
Traffic information and recommended itinerary	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Unicast/Multicast	Multi	Medium	I2V	Yes
Public transport information	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Multi	Medium	I2V	Yes
In-vehicle signage		Broadcast	Single	Medium	I2V	No
Point of Interest notification	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Multicast	Single	Low	I2V	Yes

Use case		Addressing	Hops	Frequency	Direction	Session
Automatic access control and parking management	Advertisement	Broadcast	Single	Low	I2V	No
	Service	Unicast	Single	Low	I2V/V2I	Yes
ITS local electronic commerce		Unicast	Single	Low	I2V/V2I	Yes
Media downloading		Unicast	Single	Low	I2V/V2I	Yes
Insurance and financial services		Unicast	Single	Low	I2V/V2I	Yes
Fleet management		Unicast	Single	Low	I2V/V2I	Yes
Loading zone management		Unicast/Multicast	Single	Low	I2V/V2I	Yes
Theft related services/After theft vehicle recovery		Unicast	Multi	Low	I2V/V2I	Yes
Vehicle software/data provisioning and update		Unicast	Single	Low	I2V/V2I	Yes
Vehicle and RSU data calibration		Unicast	Single	Low	I2V/V2I	Yes