TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17464

August 2020

ICS 03.220.20; 33.060.30; 35.240.60

English version

Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Security attacks modelling and definition of performance features and metrics related to security

Espace - Utilisation de la localisation basée sur les GNSS pour les systèmes de transport routiers intelligents - Modélisation des attaques de sécurité et, définition des caractéristiques de performance et des métriques liées à la sécurité

Modellierung von Sicherheitsangriffen und Definition von Leistungsmerkmalen und Sicherheitsmetriken

This Technical Report was approved by CEN on 3 February 2020. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TR 17464:2020 E

Contents

Page

European foreword

This document (CEN/TR 17464:2020) has been prepared by Technical Committee CEN-CENELEC/JTC 5 “Space”, the secretariat of which is held by DIN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Introduction

Performances of the PVT (Position, Velocity and Time) information provided by a GBPT (GNSS-Based Positioning Terminal) is a key feature that has a direct impact on the reliability and performance of the application itself. The lack of effort devoted to assess the quality of the PVT has resulted in a lack of common assessment criteria. Being able to assess the quality of a computed PVT is a critical problem for applications such Road user charging or autonomous driving.

The EC mandate M/496 ("Mandate addressed to CEN, CENELEC and ETSI to develop standardization regarding space industry") and more specifically part of the dossier 1 "Navigation and Positioning (NP) Receivers for Road Applications" of mandate M/496 (exclusion made of airport services) stressed European standards organizations to make assessment of necessary future standardization in support of the regulatory framework related to positioning performances.

The mandate work related to dossier sectorial 1, especially regarding the topics mentioned above, have been carried out by CEN/CLC TC5/WG1 and BNAE dealing with administrative management of the standardization work.

WG1 of CEN-CLC TC5 has produced draft standards EN 16803 (all parts), *Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) — Part 1: Definitions and system engineering procedures for the establishment and assessment of performances; Part 2: Assessment field tests for basic performances of GNSS-based positioning terminals; Part 3: Assessment of security performances of GNSS-based positioning terminals*.

Security of the GBPT in road Intelligent Transport Systems (ITS) became a critical point. Many applications rely on PVT information provided by GNSS. If during the past GNSS SIS attacks were considered as feasible but requiring significant technical means, it is not the case today considering that a spoofing attack can be led with a COTS SDR at relatively low cost and that jammer are available on the market at a wealth of prices.

In this context, receiver manufacturers began to implement new technologies fighting against SiS (Signal in Space) GNSS attacks and major advances that have been done in the GNSS security aspects in Europe associated to the new capabilities of the Galileo system in particular in the definition of the public regulated service and the commercial authentication service in E6 where some member of this consortium has been especially active.

1 Scope

The objective is to analyse the security issues that can occur at the GNSS SIS level. In order to do so, a full taxonomy of the GNSS SIS attacks are proposed and GNSS SIS attack security model are elaborated and classified. Security metrics for the validation of the GBPT robustness performances are defined.

The proposed methodology for this technical report consists in three distinct steps that are described hereunder:

— The first step consists in providing a full taxonomy of the possible GNSS Signal in Space attacks (voluntary or not) to be considered and identify their impact at GBPT level;

— The second step consists in regrouping narrow sets of previously identified GNSS SIS attacks into security attack models. For each security attack model, an assessment of the dangerousness based on beforehand identified key parameters and methodology will be provided;

— The third step consists in providing definition of performance objectives, security control, security metrics, and a specific procedure for a robustness evaluation of a GBPT against the identified security attack models at step II.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ETSI TS 103 246-3:2015, *Satellite Earth Stations and Systems (SES) — GNSS based location systems — Part 3: Performance requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ETSI TS 103 246-3 and ISO/IEC 27001 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
objective
result to be achieved

3.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

3.3
availability
property of being accessible and usable upon demand by an authorized entity