ETSI TR 133 926 V14.0.0 (2017-04)

TECHNICAL REPORT

LTE;
Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
(3GPP TR 33.926 version 14.0.0 Release 14)

Reference

RTR/TSGS-0333926ve00

Keywords

LTE,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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

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.

Contents

Intellectual Property Rights 2
Foreword....2
Modal verbs terminology....2
Foreword....5
1 Scope 6
2 References 6
3 Definitions and abbreviations....6
3.1 Definitions....6
3.2 Abbreviations 6
4 Generic Network Product (GNP) class description....7
4.1 Overview 7
4.2 Minimum set of functions defining the GNP class....8
4.3 Generic network product model 8
4.3.1 Generic network product model overview....8
4.3.2 Functions defined by 3GPP 8
4.3.3 Other functions 8
4.3.4 Operating System (OS)....8
4.3.5 Hardware 8
4.3.6 Interfaces....9
4.4 Scope of the present document....9
4.4.1 Introduction....9
4.4.2 Scope regarding GNP functions defined by 3GPP 10
4.4.3 Scope regarding other functions 10
4.4.4 Scope regarding Operating System (OS)....10
4.4.5 Scope regarding hardware 10
4.4.6 Scope regarding interfaces....10
5 Generic Assets and Threats 10
5.1 Introduction 10
5.2 Generic critical assets 10
5.3 Generic threats....11
5.3.0 Generic threats format 11
5.3.1 Introduction....11
5.3.2 Threats relating to 3GPP-defined interfaces 12
5.3.3 Spoofing identity 12
5.3.3.1 Default Accounts....12
5.3.3.2 Weak Password Policies 12
5.3.3.3 Password peek....13
5.3.3.4 Direct Root Access....13
5.3.3.5 IP Spoofing 13
5.3.3.6 Malware 13
5.3.3.7 Eavesdropping....13
5.3.4 Tampering....14
5.3.4.1 Software Tampering....14
5.3.4.2 Ownership File Misuse 14
5.3.4.3 External Device Boot 14
5.3.4.4 Log Tampering....14
5.3.4.5 OAM Traffic Tampering....14
5.3.4.6 File Write Permissions Abuse 15
5.3.5 Repudiation....15
5.3.5.1 Lack of User Activity Trace....15
5.3.6 Information disclosure 15
5.3.6.1 Poor key generation....15
5.3.6.2 Poor key management 15

5.3.6.3 Weak cryptographic algorithms 16
5.3.6.4 Insecure Data Storage 16
5.3.6.5 System Fingerprinting....16
5.3.6.6 Malware 16
5.3.6.7 Personal Identification Information Violation....17
5.3.6.8 Insecure Default Configuration....17
5.3.6.9 File/Directory Read Permissions Misuse 17
5.3.6.10 Insecure Network Services....17
5.3.6.11 Unnecessary Services....17
5.3.6.12 Log Disclosure 18
5.3.6.13 Unnecessary Applications....18
5.3.6.14 Eavesdropping....18
5.3.6.15 Security threat caused by lack of GNP traffic isolation 18
5.3.7 Denial of service 19
5.3.7.1 Compromised/Misbehaving User Equipments....19
5.3.7.2 Implementation Flaw 19
5.3.7.3 Insecure Network Services....19
5.3.7.4 Human Error 19
5.3.8 Elevation of privilege....20
5.3.8.1 Misuse by authorized users 20
5.3.8.2 Over-Privileged Processes/Services....20
5.3.8.3 Folder Write Permission Abuse 20
5.3.8.4 Root-Owned File Write Permission Abuse 20
5.3.8.5 High-Privileged Files 20
5.3.8.6 Insecure Network Services....21
5.3.8.7 Elevation of Privilege via Unnecessary Network Services 21

Annex A: Aspects specific to the network product class MME 22

A.1 Network product class description for the MME 22
A.1.1 Introduction 22
A.1.2 Minimum set of functions defining the MME network product class 22

A.2 Assets and threats specific to the MME 22

A.2.1 Critical assets....22
A.2.2 Threats related to AKA procedures....23
A.2.2.1 Access to 2G....23
A.2.2.2 Resynchronization 23
A.2.2.3 Failed Integrity check of Attach message....23
A.2.2.4 Forwarding EPS authentication data to SGSN 23
A.2.2.5 Forwarding unused EPS authentication data between different security domains....23
A.2.3 Threats related to security mode command procedure....24
A.2.3.1 Bidding Down....24
A.2.3.2 NAS integrity selection and use....24
A.2.3.3 NAS NULL integrity protection 24
A.2.3.4 NAS confidentiality protection....24
A.2.4 Threats related to security in Intra-RAT mobility 24
A.2.4.1 Bidding down on X2-Handover....24
A.2.4.2 NAS integrity protection algorithm selection in MME change 25
A.2.5 Threats related to security in Inter-RAT mobility 25
A.2.5.1 2G SIM access via idle mode mobility....25
A.2.5.2 2G SIM access via handover....25
A.2.5.3 2G SIM access via SRVCC 25
A.2.6 Threats related to release of non-emergency bearer 25

Annex B: Change history 27

History 28

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

[3] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

GNP Class (**Generic Network Product Class):** generic network product class is a class of network products that all implement a common set of 3GPP-defined functionalities for that particular network product

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

GNP	Generic Network Product
SCAS	Security Assurance Specification
SECAM	Security Assurance Methodology