ETSI TR 103 087 V1.2.1 (2017-11)

TECHNICAL REPORT

Reconfigurable Radio Systems (RRS);
Security related use cases and threats

Reference

RTR/RRS-0313

Keywords

radio, safety, 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

Contents

Intellectual Property Rights

Essential patents

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

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.

Introduction

The present document presents a security threat analysis of RRS networks and devices for a set of specific use cases and operational scenarios defined in ETSI TC RRS.

It is recommended to consider [i.1], [i.2], [i.3], [i.5], [i.6], [i.7], [i.8] and [i.18] for further information on the framework related to the solutions in the present document.

1 Scope

The present document provides an analysis of the risk of security attacks on the operation of reconfigurable radio systems. It identifies which security threats can disrupt RRS networks and devices or can induce negative impacts on other radio communication services operating in the same radio spectrum. The present document also identifies stakeholder and assets, which can be potentially impacted by the security threats.

The present document extends the set of use cases addressed over those covered by ETSI TR 103 087 (V1.1.1) [i.30] to cover the following:

- Remote attestation of the Reconfigurable Equipment status (installed RA and DoC).
- Configuration enforcement of reconfigurable equipment.
- Distribution and enforcement of mobility policies.
- Long-term management of devices (in particular orphaned devices).
- Secure device root of trust.

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] Recommendation ITU-T E.408: "Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. Telecommunication networks security requirements".

[i.2] L. B. Michael, M. J. Mihaljevic, S. Haruyama and R. Kohno: "A framework for secure download for software-defined radio", IEEE Communications Magazine, July 2002.

[i.3] A. N. Mody, R. Reddy, T. Kiernan and T.X. Brown: "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard", Military Communications Conference, 2009. MILCOM 2009. IEEE, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[i.4] Document Id: WINNF-08-P-0013: "Wireless Innovation Forum's Security Working Group. Securing Software Reconfigurable Communications Devices".

[i.5] ETSI TR 103 062: "Reconfigurable Radio Systems (RRS); Use Cases and Scenarios for Software Defined Radio (SDR) Reference Architecture for Mobile Device".

[i.6] ETSI TR 102 907: "Reconfigurable Radio Systems (RRS); Use Cases for Operation in White Space Frequency Bands".

[i.7] ETSI TR 103 063: "Reconfigurable Radio Systems (RRS); Use Cases for Reconfigurable Radio Systems operating in IMT bands and GSM bands for intra-operator scenarios".

[i.8] ETSI TR 102 944: "Reconfigurable Radio Systems (RRS); Use Cases for Baseband Interfaces for Unified Radio Applications of Mobile Device".

[i.9] ETSI TS 102 165-1 (V4.2.3): "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.10] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.11] ETSI EN 302 969: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices".

[i.12] ETSI TS 103 436: "Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios".

[i.13] ETSI EN 303 095: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.14] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.15] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance.

[i.16] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (Text with EEA relevance).

[i.17] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

NOTE: Available at http://eur-lex.europa.eu/.

[i.18] ETSI TR 102 967: "Reconfigurable Radio Systems (RRS); Use Cases for dynamic equipment reconfiguration".

[i.19] ETSI EN 303 146-2: "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)".

[i.20] ETSI TS 103 146-3: "Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols Part 3: Unified Radio Application Interface (URAI)".

[i.21] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.22] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.23] ETSI TS 103 146-4: " Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols; Part 4: Radio Programming Interface (RPI)".

[i.24] Open Mobile Alliance™ OMA-ERP-DM-V1_3: "OMA Device Management".

NOTE: Available at http://www.openmobilealliance.org/.

[i.25] Open Mobile Alliance™ OMA-ERP-LightweightM2M-V1_0: "OMA LightweightM2M (LWM2M)".

NOTE: Available at http://www.openmobilealliance.org/.

[i.26] GSM Association RCC.14 : "Service Provider Device Configuration".

[i.27] ETSI TR 103 502: "Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks Security aspects".

[i.28] Trusted Computing Group: "Trusted Platform Module Library, Part 1: Architecture, Family '2.0'".

[i.29] Trusted Computing Group: "TPM Main, Part 1, Design Principles".

NOTE: Available at https://trustedcomputinggroup.org/.

[i.30] ETSI TR 103 087 (V1.1.1): " Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems".

[i.31] IEEE 802.11™: "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.32] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

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

assigned frequency band: frequency band or sub-band within which the device is authorized to operate and to perform the intended function of the equipment

National Regulatory Authority (NRA): body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives (Framework Directive 2002/21/EC [i.21])

radio system: system capable to communicate some user information by using electromagnetic waves

NOTE: Radio system is typically designed to use certain radio frequency band(s) and it includes agreed schemes for multiple access, modulation, channel and data coding as well as control protocols for all radio layers needed to maintain user data links between adjacent radio devices.

RE Configuration Policy: machine-readable document that is generated by the RE manufacturer or its representative (such as the Conformity Contact Entity) (such as the Conformity Contact Entity), and which contains instructions that are relevant for the RE to maintain compliance to the RED (for example, valid hardware and software combinations)

NOTE: Security objectives regarding to the DoC should be understood as applying both to the DoC and the RE Configuration Policy. Procedures that involve decision making based on the DoC implicitly use the RE Configuration Policy.

Reconfigurable Radio System (RRS): radio system using reconfigurable radio technology

security threat: potential violation of security

NOTE: Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

use case: description of a system from a user's perspective

NOTE 1: Use cases treat a system as a black box, and the interactions with the system, including system responses, are perceived as from outside the system. Use cases typically avoid technical jargon, preferring instead the language of the end user or domain expert.

NOTE 2: Use cases should not be confused with the features/requirements of the system under consideration. A use case may be related to one or more features/requirements; a feature/requirement may be related to one or more use cases.

NOTE 3: A brief use case consists of a few sentences summarizing the use case.

user: user of the Mobile Network

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASF	Administrator Security Function
CA	Certificate Authority
CCE	Conformity Contact Entity
CE	Conformité Européenne
CIAAA	Confidentiality, Integrity, Authentication, Availability, and Accounting
CM	Configuration Manager
CoAP	Constrained Application Protocol
ComSec	Communication Security
CPU	Central Processing Unit
CR	Cognitive Radio
CSL	Communication Service Layer
CSP	Communication Service Provider
DAA	Download Authorization Authority
DM	Device Management
DMA	Direct Memory Access
DoC	Declaration of Conformity
DTLS	Datagram Transport Layer Security
EK	Endorsement Key
EU	European Union
GBA	Generic Bootstrapping Architecture
GNSS	Global Navigation Satellite System
GS	Group Specification
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile Communications Association
HAL	Hardware Abstraction Layer
HMAC	keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	HardWare
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IR	Intermediate Representation
IT	Information Technology
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
LTE	Long Term Evolution
LWM2M	LightWeight Machine to Machine
M2M	Machine to Machine
MAC	Medium Access Control
MCC	Mobile Country Code
MD	Mobile Device
MDRC	Mobile Device Reconfiguration Class
MNC	Mobile Network Code
MO	Management Object
MURI	MUltiRadio Interface
NFV	Network Function Virtualisation

NRA	National Regulatory Authority
OBEX	OBject EXchange
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OS	Operating System
OSI	Open System Interconnection
PCR	Platform Configuration Register
PHY	PHYsical
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QA	Quality Assurance
RA	Radio Application
RAP	Radio Application Package
RAT	Radio Access Technology
RC	Radio Controller
RCF	Radio Controller Framework
RE	Reconfigurable Equipment
RECP	Reconfigurable Equipment Configuration Policy
RED	Radio Equipment Directive
RF	Radio Frequency
RPI	Radio Programming Interface
RPOE	Radio Platform Operating Environment
RRFI	Reconfigurable Radio Frequency Interface
RRS	Reconfigurable Radio System
RRS-CP	RRS Configuration Provider
RVM	Radio Virtual Machine
SAE	System Architecture Evolution
SCA	Software Communication Architecture
SCADA	Supervisory Control And Data Acquisition
SCC	Standards Coordination Committee
SCP	Software/Content Provider
SD	Software Distributor
SDR	Software Defined Radio
SDRD	Software Defined and Reconfigurable Devices
SFB	Standard Functional Block
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPA	Service Provider Application
SPDC	Service Provider Device Configuration
SW	Software
SWIR	Software Intermediate Representation
TAD	Transfer of Authority Document
TLS	Transport Layer Security
TLV	Type-Length-Value
TOE	Target Of Evaluation
TPM	Trusted Platform Module
TR	Technical Report
TRNG	True Random Number Generator
TVRA	Threat Vulnerability Risk Analysis
UA	User Application
UDFB	User Defined Functional Block
UDP	User Datagram Protocol
UML	Unified Model Language
URA	Unified Radio Application
URAI	Unified Radio Application Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Unique Reference Number
USB	Universal SErial Bus