ETSI TR 103 502 V1.1.1 (2017-09)

TECHNICAL REPORT

Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks; Security aspects

Reference

DTR/RRS-0314

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

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.

Executive summary

The introduction of RRS capability is shown not to inhibit the provision of the security mechanisms of existing radio access technologies. The reason, shown in the present document, is that the security capabilities for common radio technologies (e.g. LTE/SAE, IEEE 802.11™) are present at layers 2 and higher in the OSI protocol stack, whereas the novel features of RRS apply to the means to provision layer 1. It is highlighted however that a Radio Application addresses a complete protocol stack and provision of all layers of the protocol stack in a single software package may require special provisions in the Reconfigurable Equipment to enable full network communication.

1 Scope

The present document shows a mapping of existing Radio Access Technologies (RATs) to the Reconfigurable Radio System (RRS) model in order to identify missing security requirements, in particular identify the boundary of an RRS Radio Application with regard to the security functions present in existing RAT. Recognizing that a RAT is not bound to a single link but may be supported by functions in the network the present document also considers the role of core networks in supporting any triggering of the Reconfigurable Equipment to reconfigure itself using a push mechanism.

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 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[i.2] ISO/IEC 7498-1:1994 "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model".

[i.3] ETSI TR 102 945: "Reconfigurable Radio Systems (RRS); Definitions and abbreviations".

[i.4] ETSI EN 303 095: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.5] Len Sassaman, Meredith L. Patterson, Sergey Bratus, Michael E. Locasto, Anna Shubina: "Security Applications of Formal Language Theory".

[i.6] Noam Chomsky: "On certain formal properties of grammars", Information and Computation/information and Control, vol. 2, pp. 137-167, 1959.

[i.7] Michael Sipser: "Introduction to the Theory of Computation", Second Edition, International Edition, Thompson Course Technology, 2006.

[i.8] Seymour Ginsburg and Sheila Greibach: "Deterministic context free languages", in Proc. 6th Symp. Switching Circuit Theory and Logical Design, 1965, pp. 203-220.

[i.9] Dan Kaminsky, Meredith L. Patterson and Len Sassaman: "PKI Layer Cake: New Collision Attacks Against the Global X.509 Infrastructure".

[i.10] Travis Goodspeed, Sergey Bratus, Ricky Melgares, Rebecca Shapiro and Ryan Speers: "Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios", 5th USENIX Workshop on Offensive Technologies, August 2011.

[i.11] Open Mobile Alliance™. OMA-AD-Push-V2-3: "Push Architecture".

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