Radiocommunication Study Groups

Received: 16 February 2016

Subject: ITU-R Report [IMT-2020.TECH PERF REQ]

Document 5D/XX-E
16 February 2016
English only

FRANCE

NEW PROPOSAL ABOUT REQUIREMENT AND EVALUATION CRITERIA OF TECHNOLOGIES TO ENHANCE SECURITY AND PRIVACY OF RADIO-COMMUNICATIONS

1 Introduction

In order to address evolving user needs, ITU-R is currently working on the future development of "IMT for 2020 and beyond". In this context, the WP 5D elaborated the Recommendation ITU-R M.2083 which identifies at § 2.3.8 and § 5:

- Needs for robust and secure technologies to counter the threats to security and privacy brought by new radio technologies, new services and new deployment cases of IMT systems.
- Privacy requirements, such as preventing unauthorized user tracking.
- Protection requirements of network against hacking, fraud, denial of service, man in the middle attacks.
- Security requirements such as encryption and integrity protection of user data and signalling.

In addition, during the 22st meeting of Working Party 5D held in San Diego, California, USA from 10 18 June 2015, the work on a draft new Report ITU-R M.[IMT-2020.TECH PERF REQ] - Requirements related to technical performance for "IMT-2020" radio interface technologies, has been started.

As far as security and privacy are concerned, several vulnerabilities of public wireless networks are relevant to some lacks of protection of the messages that are exchanged during the network access (see Annex 1 for examples). In order to cover these issues for the sake of efficient system design, economy of scale and facilitated deployment of IMT 2020 systems:

- a way could be to use the radio propagation environment to try to develop "security of the radio access",

- the different security items should be addressed, e.g. :

  - System signalling integrity and confidentiality
  - Mutual authentication between UE and system/network, and perhaps between home and serving network
  - Subscriber identity authentication
  - Subscriber identity confidentiality

- User data integrity and confidentiality

Thus, it is desirable to agree on the technical operational and performance indication parameters of IMT 2020 systems and technologies, including those dealing with security of the radio access and privacy of the subscriber, by considering the different protocols layers and by considering different security functions.

2 Proposals

France proposes to consider

- the material describing examples of security weakness in annex 1
- a section in the table of contents of the report which addresses the secure & privacy issues [IMT-2020.TECH PERF REQ] as described in annex 2. Note that annex 2 provides two possible approaches for consideration by the WP 5D.
    - the first approach focuses on security and privacy requirements from the protocol layers and the relevant risks side (eavesdropping and radio hacking at physical layer, cyber-attack at upper layers).
    - the second approach focuses on security and privacy requirements from the main security functions side (from system signalling integrity to user data confidentiality).

Annex 1

EXAMPLES OF SECURITY WEAKNESS

As an example of security weaknesses, the following figures briefly analyse the EPS–AKA procedure and the key management involved in 3G and 4G RATs, and they explicit some of the relevant vulnerabilities. More details can be found in the following references below.

[1] "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA » Ref: Hyeran Mun, Kyusuk Han and Kwangjo Kim1-4244-2589-1/09/2009 IEEE,

[2] F. Delaveau and ali "Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures – an overview" Winncomm Forum Europe 2013. «http://www.phylaws-ict.org/?page_id=92» [On line]

[3] Ccc-Tv, «SS7map : mapping vulnerability of the international mobile roaming infrastructure,» [On line]. Available: https://media.ccc.de/v/31c3_-_6531_-_en_-_saal_6_-_201412272300__ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira#video.

[4] T. intercept, «The Great SIM Heist, Hows Spies kept the key of the Encryption Castle» [On line]: https://firstlook.org/theintercept/2015/02/19/great-sim-heist/.

[5] EC project PHYLAWS: deliverable D.2.1 online «http://www.phylaws-ict.org/?page_id=48» [On line]

[6] Bruce Schneier "Applied Cryptography" second edition John Wiley & Sons.

First, figure 1 below points out some of the messages exchanges between User Equipment (UE), Access point or Nodes (AP), authentications servers and operators data bases. At the bottom of the figure and in red character are mentioned some of the main relevant vulnerabilities.

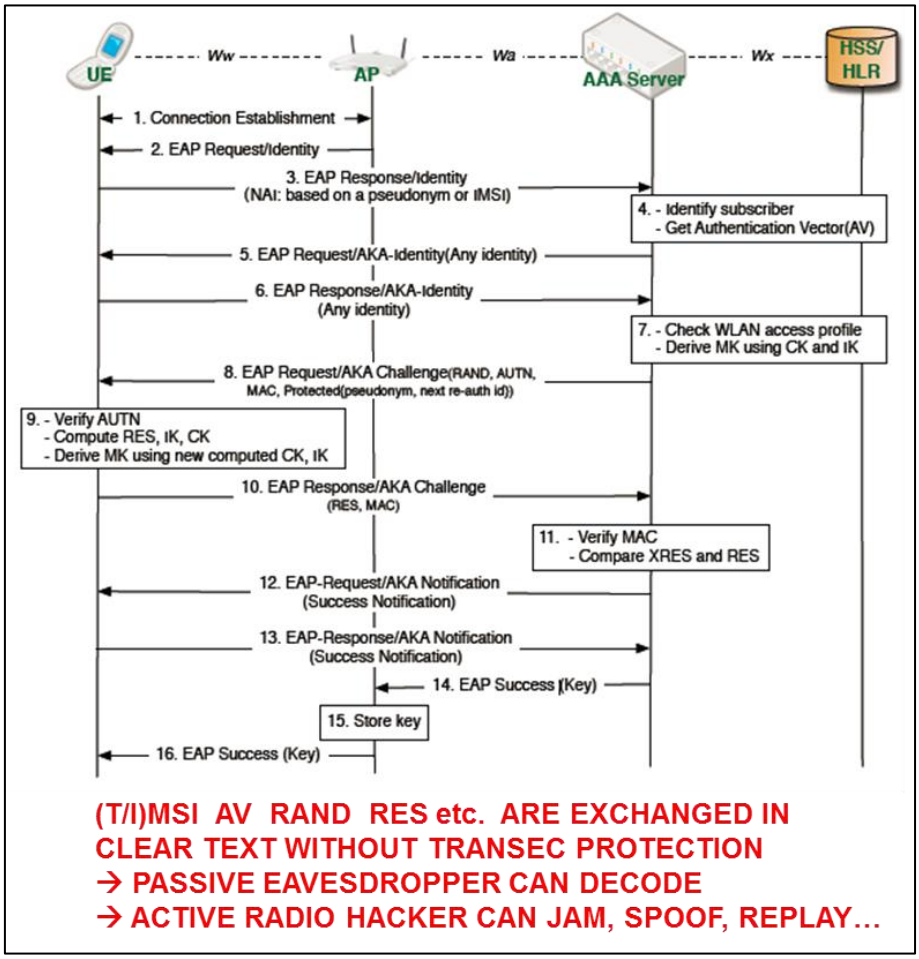

Figure 1: detail of the EPS-AKA protocols - relevant security weaknesses

From the figure above, it appears that

- Any passive radio-eavesdropper can easily monitor and decode clear text information relevant to the network access before encryption ciphering is established ([2]). This applies to network's signalling, subscriber pseudonyms, subscribers' identities when transmitted, content of request and response messages, authentications vectors, etc.
- Active radio-hacking systems can lead replays attacks, man in the middle and impersonating attacks into the exchanged messages, in order to influence the roaming protocol, the authentication protocol and the cipher establishment. For example, this may lead to the disclosure of IMSI and IMEI of UE. Moreover, the disclosure of the subscriber's Key K may be achieved when the radio-hacker combines the exploitation of weaknesses of the authentication protocol at the physical layer [2] and of failures of the SS7 protocol used in the international roaming [3]).

Second, figure 2 below point out the dependency of integrity and encryption keys computed by User Equipment (UE) and e-Nodes: the algorithms are public and all keys are derived from a single subscriber Key K which shall remain secret. Unfortunately, recent news highlighted serious disclosure of K keys by several means [3,4]. Then, from the knowledge of the subscriber key K, a passive eavesdropper can monitor the exchanged request and response messages between a node and a terminal, compute exactly the same keys, then monitor all stages of the network access protocol and monitor any exchanged messages. Similarly, a radio hacker (informed of the K key) could intrude the message and impersonated both the node and the terminal at any stage of the network access and when user data traffic is established.

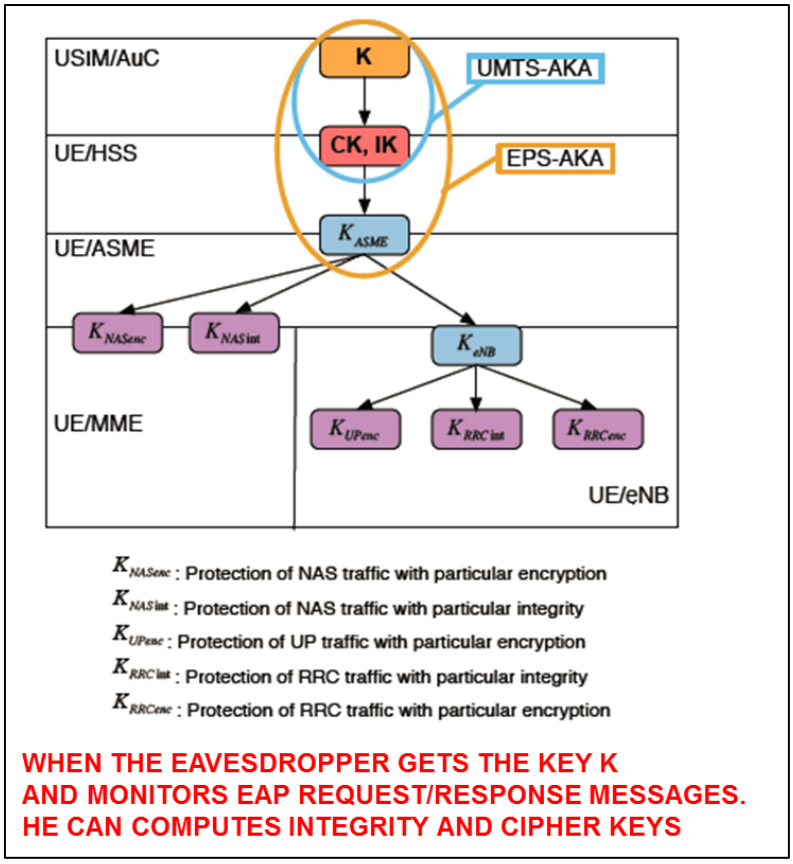

Figure 2: derivation of integrity and encryption keys from the subscriber key K

In addition, it is noticeable that secret encryption algorithm has no real practical efficiency for wireless public RATs, since the (secret) algorithms are often disclosed after a few years, as it happened for the A3 A8 and A5 algorithms designed into the GSM standard [6].

Annex 2

PROPOSALS FOR ENTRIES INTO THE REPORT IMT-2020.TECH PERF REQ

For the building of the report [IMT-2020.TECH PERF REQ], two possible approaches are proposed for consideration by the WP 5D.

A/ The first approach focus on security and privacy requirements by considering the different protocol layers and the relevant risks (physical layer being vulnerable to eavesdroppers and radio hackers and upper layer being vulnerable to cyber-attackers)

1.1. REQUIREMENT AND EVALUATION CRITERIA FOR TECHNOLOGIES TO ENHANCE PRIVACY AND SECURITY
- 1.1.1. Security of the physical layer
  - 1.1.1.1. SIM/UIM based security at the physical layer
  - 1.1.1.2. Physical layer based security
  - 1.1.1.3. Merge of previous technologies
  - 1.1.1.4. Evaluation
  - 1.1.1.5. Required KPI
- 1.1.2. Security of the upper layers
  - 1.1.2.1. SIM/UIM based security at upper layers
  - 1.1.2.2. Input of physical layer security into upper layers
  - 1.1.2.3. Evaluation
  - 1.1.2.4. Required KPI
- 1.1.3. Overall evaluation and conclusion

B/ The second approach focus on security and privacy requirements by considering the main security functions over all protocol layers

1.2. REQUIREMENT AND EVALUATION CRITERIA FOR TECHNOLOGIES TO ENHANCE PRIVACY AND SECURITY
- 1.2.1. System signalling integrity and confidentiality
  - 1.2.1.1. Required KPIs
  - 1.2.1.2. Solutions 1
  - 1.2.1.3. Solution n
  - 1.2.1.4. Evaluation
- 1.2.2. Mutual authentication between UE and system/network
  - 1.2.2.1. Required KPIs
  - 1.2.2.2. Solutions 1
  - 1.2.2.3. Solution n
  - 1.2.2.4. Evaluation
- 1.2.3. Mutual authentication between home and serving network
  - 1.1.1.1. Required KPIs
  - 1.1.1.2. Solutions 1
  - 1.1.1.3. Solution n
  - 1.1.1.4. evaluation
- 1.2.4. Subscriber identity authentication
  - 1.2.4.1. Required KPIs