5G-ENSURE

(Project Number— 671562)

Security focus in 5G standardization

1st 5G-ENSURE INTERNATIONAL WORKSHOP ON STANDARDISATION
5G Enablers for network and system security and resilience

16 June 2016

Paolo DE LUTIIS
TIM INFORMATION TECHNOLOGY

This research has been performed within 5G-ENSURE project (www.5GEnsure.eu) and received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 671562.

Outline of the presentation

- Focus on 5G-ENSURE Project strategy
- Project objectives about standardization
- Standardization Plan
- Main activities and main results achieved
- Next steps

Standardization objectives

- Monitoring standardisation activities directly related to the 5G-ENSURE research topics ensuring the overall coherence of the project results and understanding where the project can contribute to 5G Security specification
- Transferring project results to relevant standards bodies
- Facilitating joint contributions and building consensus (e.g. improving the number of co-signed contributions) taking into account protection of IPR, company policy, marketing issues, etc.
- Participating to 5G-PPP pre-standard group for joint activities and build pre-standardization consensus
- Receive feedback on 5G security and privacy challenges, priorities, solutions required and to understand how to drive 5G standardisation to ensure that security is correctly addressed
  - Organizing international workshops to present relevant project results and to ensure 5G-ENSURE visibility to a wide audience
  - Launch a 5G-ENSURE Public consultation on 5G security to collect the different views on 5G security.

Relevant topics for 5G Security

Potentially all the 5G-ENSURE deliverables contains topics to be standardised. In particular (1st and subsequent iterations of the documents):

- Use-Cases (D2.1 public since M03)
- Trust model and Security Requirements (D2.2 & D2.3 due to M08)
- Security Architecture (D2.4 “draft” due to M12)
- Enablers (D3.1 “early vision” public since M04):
  - AAA
  - Privacy
  - Trust
  - Security Monitoring
  - Network Management & Virtualization isolation

Standardization Plan

5G-ENSURE Research Topics	Targeted Standards Groups
5G security specific use cases **5G Trust Model** **5G security requirements** **5G security architecture** **AAA GE & Privacy GE**	TSG Service and System Aspects (TSG-SA) group SA WG2 Architecture SA WG3 – Security RAN – Radio Access Network
Network Management & Virtualisation isolation GE **Security Monitoring GE** **AAA GE** **Privacy GE**	Network Functions Virtualisation (NFV ISG) Technical Committee (TC) Cyber Security (CYBER) Technical Committee Smart Card Platform (TC SCP)
Network Management & Virtualisation isolation GE	OpenFlow™ and SDN
AAA GE **Network Management & Virtualisation isolation GE**	Authentication and Authorization for Constrained Environments (ACE) Network Functions Virtualisation Research Group (NFVRG)
5G Trust Model **5G Security requirements**	Security and Fraud Risk Assessment (SFRA)

3GPP is the main target

- SA1 (Requirements). SMARTER (TR 22.891) branches:
  - TR 22.861 Massive Internet of Things (mIoT)
  - TR 22.862 Critical Communications (CRIc)
  - TR 22.863 Enhanced Mobile Broadband (eMBB)
  - TR 22.864 Network Operation (NEO)
- SA2 (Architecture): TR 23.799 Study on Architecture for Next Generation System
- SA3 (Security):TR 33.899 Study on the security aspects of the next generation system
- RAN plenary: TR38.913 Study on Scenarios and Requirements for Next Generation Access Technologies

Direct Contributions

- SA3 (Security):TR 33.899 Study on the security aspects of the next generation system
  - Enablers (as security areas): AAA, Privacy, etc.
- 3GPP RAN plenary: TR 38.913 Study on Scenarios and Requirements for Next Generation Access Technologies
  - Requirements
- ETSI TC Cyber:
  - nWI proposal on «Access control enforcement mechanisms and policy rules for PII protection on smart devices, cloud and Mobile Services»
  - (Proposed) extension of the current TR 103.304 «PII Protection in mobile and cloud services» with specific 5G Privacy needs descriptions

Next steps

- Review of the standardization plan depending on the results of this workshop and the open consultation survey.
- Provide additional contributions toward SA3 about Study Item on Study on Security aspects of the next generation system (TR 33.899) and TC Cyber on privacy (TR 103.304 and the possible new TS)
- Try to reach directly other groups/SDO (e.g. ETSI ISG NFV, etc.)
- Identify additional outcomes to standardize, as soon as the official deliverables of the project will be ready (e.g. Requirements, Architecture, Enablers)

Thanks.

QUESTIONS ?