ENABLERS FOR A SECURE AND RESILIENT 5G

Martin Svensson
SICS Security Lab

Follow us @SICS_SwedishICT
WHY DOES 5G NEED NEW ENABLERS?

• Support new use cases and business models

• Mitigate new threats and address revealed weaknesses
5G-ENSURE (H2020)

The reference project for 5G Security, Privacy and Trust

• Produce a 5G Security architecture and Use Cases
• An initial set of Security Enablers
• 5G Security test bed
• Contribute to standards bodies
PROPOSALS FROM 5G-ENSURE

AAA – *Impact*: 5G support for IoT and satellite systems & enable trust and liability levels

Privacy – *Impact*: creation of services and business models on top of 5G

Trust – *Impact*: trustworthy dynamic 5G multi-stakeholder system

Security Monitoring – *Impact*: Resilient 5G system to implement new services

AAA AUTHENTICATION – AUTHORIZATION – ACCOUNTING

Rationale behind the enablers:

• *Increased flexibility*
• *Internet-of-Things*
• *Lightweight protocols*
• *Enhanced security features*
AAA  AUTHENTICATION – AUTHORIZATION – (ACCOUNTING)

Features introduced by 5G-ENSURE:
• **USIM-less devices**
• **Authentication based on 3rd party identities (BYOI)**
• **Group-based authentication**
• **Integration of existing AAA protocols in satellite and terrestrial**

• **(Perfect) Forward secrecy**
• **Trusted Interconnect between operator networks**
Increase users’ **assurance** and **confidence** in 5G

- **User and device identity privacy**
- **Location privacy**
- **Communication privacy**
- **Data privacy**

By a proactive, privacy-by-design approach
PRIVACY

Features introduced by 5G-ENSURE:

• Improved protection of the identities
  • Both 3GPP and non-3GPP access (WiFi/EAP-SIM)
  • Protection against identity disclosure and location leaks
• End-to-End encryption
TRUST

• **Trust**: a quantifiable but subjective measure of a trustor’s belief that a system will produce acceptable outcomes.

• **Trustworthiness** (of a socio-technical system): its ability to produce outcomes acceptable to all trustors.
TRUST

Establishes a new trust model, addressing:

• *Trust between automated systems* (*M2Mt*)
• *Trust between human stakeholders* (*U2Ut*)
• *Trust that a human stakeholder has towards a system* (*U2Mt*)
• *Trust that an automated system has in its users* (*M2Ut*)
SECURITY MONITORING

Security by operation solutions to ensure the highest level of security and resilience

- Virtualized (SDN / NFV) infrastructure
- Dynamic topologies
- Massive IoT
SECURITY MONITORING

Features introduced by 5G-ENSURE:

• System security state repository
• Satellite network monitoring
• PulSAR - Proactive Security Analysis and Remediation
Goal of enablers:

• Securing a network’s control plane and the virtualized networks on top of it

• Securing network services and providing new security services
NETWORK MANAGEMENT & VIRTUALISATION ISOLATION

Features introduced by 5G-ENSURE:

• Anti-fingerprinting in software defined networks
• Bootstrapping trust
• Micro-segmentation in 5G
5G-ENSURE SECURITY ENABLERS

Technical roadmap released in March 2016

Open specification will be released in June 2016

Software release 1 scheduled for October 2016
CONCLUSION

• Enablers will address security in 5 areas
  • 22 individual enablers will be released
  • Supported by the (security) use cases

• An open specification will be made available

• Enables new (security) functionality and address known weaknesses
READ MORE

- 5G-ENSURE Deliverables: http://5gensure.eu/deliverables

- 5G: Towards secure ubiquitous connectivity beyond 2020: http://soda.swedishict.se/5933/