5G Activites of NGMN

Security Competence Team (SCT)

ITU Workshop on 5G Security
Geneva, 19 March 2018

Mission

Security Competence Team (SCT) formed in May 2017

- *Provide vision and high-level security and privacy requirements for NGMN, with respect to both digital infrastructure and verticals*
- *Interact with standardization and other relevant organizations*
- *Provide input to other NGMN work groups*
- Promote business opportunities and improved user experience
- Take holistic security approach, in addition to communications security (3GPP) approach
- Promote security and privacy by design and integrated cybersecurity

Challenges

- Network virtualization and slicing together with E2E framework and massive IoT require a holistic approach to security including software and hardware security aspects in addition to traditional network security aspects
- Lawful access needs to be separated from unlawful access; privacy-sensitive data need to be protected (e.g., IoT data in E2E manner, possibly at applications or communications layer)
- There is an overlap with non-NGMN security groups, in terms of security areas and participating companies
- Standardization organizations (e.g., 3GPP SA3) focus on more specific requirements and concrete solutions
- Consequently, the right balance between high-level NGMN requirements and more concrete standardization requirements is needed in order to increase practical impact of NGMN

SCT Activities (Overview)

- **5G E2E Architecture Framework** – Security requirements
- **Cellular V2X** – Security and privacy aspects
- **Network Capabilities Exposure** – Security aspects and requirements
- **5G RAN Functional Decomposition** – Security of new interfaces
- **Update** of "**5G Security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience**" (NGMN, Oct. 2016) with respect to law enforcement requirements for MEC
- **Pre-commercial 5G Network Trials & Testing** – Security Tests

SCT Activities (1)

- **5G E2E Architecture Framework** – Security requirements

- E2E architecture framework necessitates a wide range of security requirements, concerning network layer, business enablement layer, business application layer, management and orchestration, endpoint/user equipment, as well as identity management

- *White paper (v1.0 and v2.0), with SCT input, published and distributed with liason statements to 3GPP TSG SA WG3, ETSI SAGE, ETSI TC CYBER, ISO/IEC JTC1/SC 27, FIDO Alliance, etc.*

SCT Activities (2)

- **Cellular V2X** – Security and privacy aspects

- Comparison of network-layer security in LTE V2X and 802.11p as well as of application-layer security in IEEE/SAE (with SCMS) and ETSI ITS
- LTE interfaces to be used: LTE PC5 (network-supported or not) and LTE Uu (with eMBMS)
- Privacy considerations, especially w.r.t. tracking and linkability
- ***Advantages of LTE V2X over 802.11p pointed out***
- ***White paper, with SCT input, to be published soon***

SCT Activities (3)

- **Network Capabilities Exposure** – Security aspects and requirements

- Exposure of network access and communications services and functions, network infrastructure, and their management to 3rd parties
- Security requirements, exposure of security capabilities, scenarios, and use cases
- *White paper to be finalized soon*

SCT Activities (4)

- **5G RAN Functional Decomposition** – Security of new interfaces

➢ *White paper, with SCT input on F1 interface, published; dedicated SCT security document in preparation*

- **Update** of “**5G Security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience**” (NGMN, Oct. 2016) with respect to law enforcement requirements for MEC

➢ *Updated white paper published and distributed*

- **Pre-commercial 5G Network Trials & Testing** – Security tests

➢ To start soon

SCT Relationships

- **3GPP:** SA3, SA2, SA1, SA5, RAN, etc
- **ETSI:** TC LI, SAGE, TC CYBER, ISG NFV, ISG MEC, etc
- **ISO/IEC:** JTC1/SC 27
- **5GAA**
- **GSMA**
- **FIDO Alliance**
- **… and many more including ITU**

NGMN SCT welcomes the feedback and involvement from ITU-T SG17

Thank you

Merci

Спасибо

谢谢

شكرا

Gracias

ありがとう

감사합니다