5G security activities and future plan in ITU-T SG17

Heung Youl Youm, PhD

Chairman, ITU-T SG17
Professor, Soonchunhyang University, Korea(Rep. of)

SOON CHUN HYANG UNIVERSITY

Content

- Strategic Vision for ITU-T SG17
- Overview of 5G security framework, including threats landscape, security components for 5G network
- Outcomes from ITU workshop on 5G security, on March 2018
- Questions in SG17 for 5G security
- Activities related to 5G Security in SG17
- Potential work items specific to 5G security in ITU-T SG17
- Conclusion and recommendations

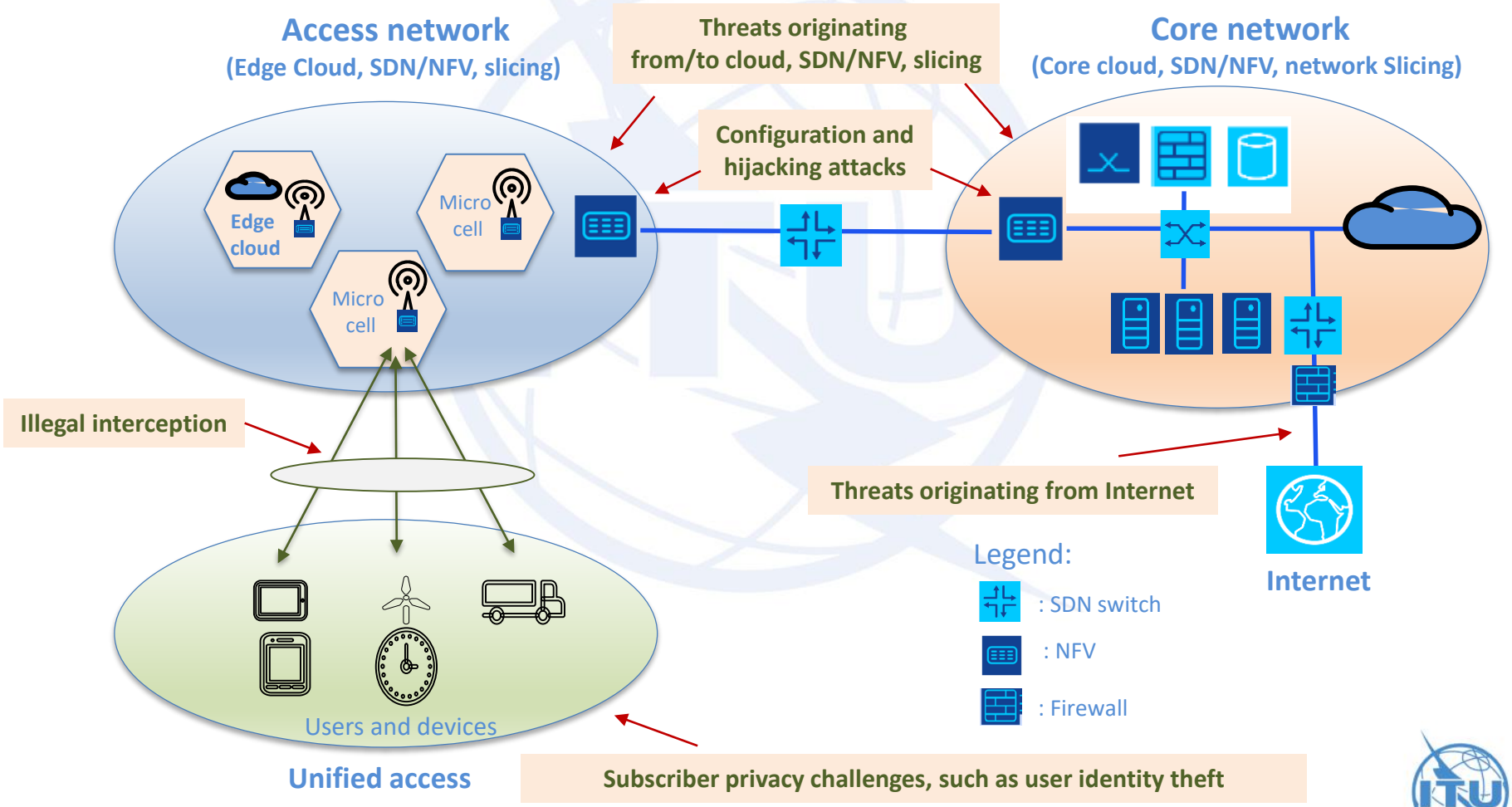
Strategic Vision for ITU-T SG17 in this study period 2017-2020

- Be a center of security competence with more participation from ITU membership
- Study new emerging areas and produce high quality technical Recommendations that are implementable
- Increase collaboration/cooperation with other international organizations

ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT).

A flexible and dependable 5G network and general threats landscape

- 5G will be built on mobile clouds, SDN, NFV, and network slicing to meet the challenges of massive connectivity, flexibility, and costs.



Exemplar threats in 5G network

Well-know threats from

- Software vulnerabilities
- Configuration mistakes and bad practices
- Flooding attacks such as DDoS attack

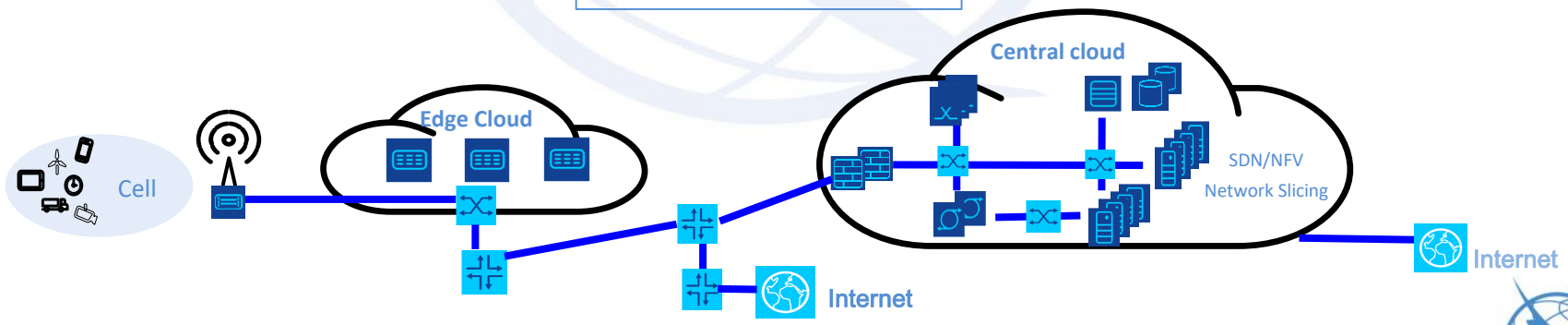
Incidents exploiting threats give higher impact on 5G services than 4G.

Network level threats

- Threats related to SDN that separate packet forwarding and control.
- Threats related to NFV that virtualizes network services run on dedicated hardware.
- Threats related to network slicing
- Threats related to cloud computing.

Infrastructure sharing

- Facilitate side channel attacks

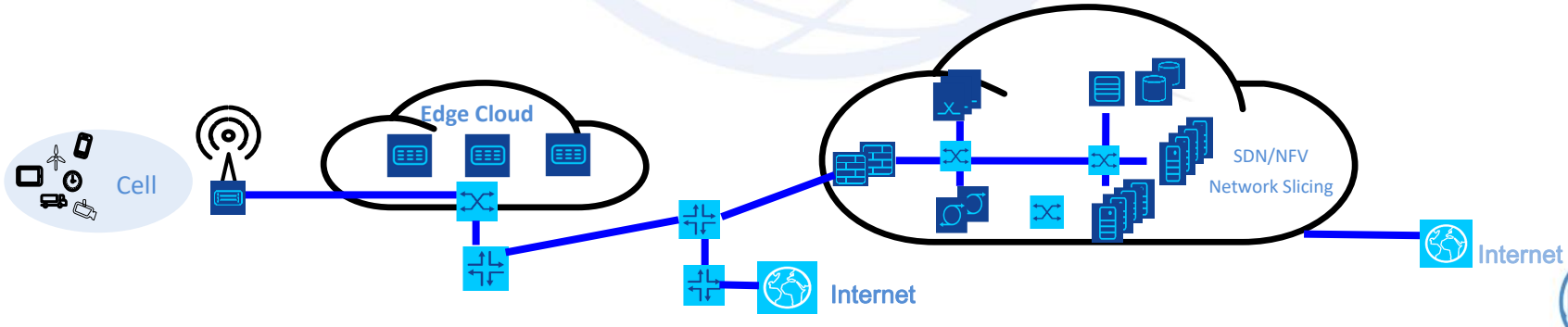


An example of security components in 5G network

UE security	AN security	CN security	Services security
▪ Subscriber/device identifier /credentials ▪ Identity security ▪ Secure hardware ▪ Enhanced user privacy	▪ Authentication/authorization, key agreement ▪ Security negotiation ▪ Enhanced subscriber privacy ▪ Mobile edge computing security	▪ Core cloud security ▪ Automation and orchestration for security ▪ Self adaptive, intelligent security controls	▪ Services security ▪ Big data analytics
	▪ SDN/NFV/network slicing security ▪ Configuration validation ▪ Access control		

Generic security enablers

- Cryptography, Public Key Infrastructure, Identity management, Threat intelligence sharing, security testing and certification
- Privacy such as location security, identity security



ITU workshop on 5G security
19 March 2018

- Workshop objectives were:
  - to better understand evolving threats landscape;
  - to identify security requirements from 5G manufacturers, telecommunication operators, regulators, and application providers;
  - to share the on-going activities among relevant groups; and
  - to identify potential directions including new topics or ongoing work requiring collaboration among relevant groups above.
- Speakers from Nokia, KT, China Mobile, Huawei, TNO, Trialog, Horst Görtz Institute, KAIST, King's College London.
- Session 4 discussed future directions and potential work items.

Workshop outcomes – future directions(1)

Takeaways and Conclusions

1. Identified standardization groups related to 5G security: NGMN Security Competence Team (SCT), 3GPP SA3, ETSI ISG NFV, GSMA, OASIS, and others (for example, IETF I2NSF, TLS, QUIC, UTA).
2. Identified SGs in ITU-T: SG11, SG13(to take the lead on 5G), SG15(transport), SG17(security aspects), Joint Coordination Activity on IMT2020 (JCA-IMT2020) under SG13, and FG-ML5G.

Suggestions to ITU-T SG17

- ❑ Collaborate with relevant groups and participate in JCA on IMT2020 for 5G security standardization work.
- ❑ Develop a standardization roadmap for 5G security and identify gaps for SG17 to study in the area of 5G security.
- ❑ Utilize trust model by 3GPP as a starting point.
- ❑ Study minimum compliance risks related to 5G applications.
- ❑ Utilize the cloud, big data and SDN infrastructure to build 5G security infrastructure.

Workshop outcomes – future directions(2)

Takeaways and Conclusions

3. Identified security subjects: Security for network slicing, NFV/SDN and Edge computing
4. Relevant Questions in SG17: Q4/17, Q9/17, Q11/17 (General issues), Q2/17(network aspects), Q6/17(infrastructure aspects), Q7/17(application aspects), Q8/17 (cloud computing security), Q11/17 (Cryptographic algorithm aspects), and Q14/17 (DLT)
5. Use multiple relevant Questions in SG17,
6. Take an orchestrated security and holistic security approach.

Suggestions to ITU-T SG17

- Study security for network infrastructure, edge cloud computing, end-to-end, and cryptographic profile: for example, security orchestration, trust concept and trust model based on PKI, DLT based PKI, IDM for 5G, multi-level certification, quantum aspects, management automation aspects using AI and machine learning, and DLT-based management.
- Ask members to submit Contributions for 5G security.
- Ask relevant Questions to identify appropriate work items for 5G security.

Questions in SG17 for 5G security

- **WP 1 "Telecom/ICT security"**
  - Q2/17 Security architecture and framework
  - Q3/17 Telecommunication information security management
  - Q6/17 Security aspects of telecommunication services, networks and Internet of Things
  - Q13/17 Security aspects for Intelligent Transport System
- **WP 2 "Cyberspace security"**
  - Q4/17 Cybersecurity
  - Q5/17 Countering spam by technical means
  - Q14/17 Security aspects for distributed ledger technologies
- **WP 3 "Application security"**
  - Q7/17 Secure application services
  - Q8/17 Cloud computing security
  - Q12/17 Formal languages for telecommunication software and testing
- **WP 4 "Identity Management & Authentication"**
  - Q9/17 Telebiometrics
  - Q10/17 Identity management architecture and mechanisms
  - Q11/17 Generic technologies to support secure applications
- **Q1/17 Telecommunication/ICT security coordination**

Newly established on March 2017.

Newly established on September 2017.

SDN/NFV/network slicing security for 5G

Lead Question on 5G

ITS security for 5G

Threats information sharing for 5G

Application and service aspects for 5G

Infrastructure security for 5G, including cloud and big data

IdM for 5G

PKI and trust management for 5G

Activities related to 5G Security in SG17 (1)

- **Q2/17 (Security architecture and framework)**
  - Network aspects including SDN for 5G security
    - X.1038 (2016): Security requirements and reference architecture for SDN
    - X.SDsec: Guideline on software-defined security in SDN/NFV network
    - X.sdnsec-3: Security guideline of service function chain based on SDN
    - X.ssc: Security service chain architecture
    - X.srnv: Security requirements of network virtualization

- **Q6/17 (Security aspects of telecommunication services, networks and IoT)**
  - Mobile and infrastructure (including IoT) aspects for 5G security
    - X.1121 - X.1127 (2004-2017) on Mobile security
    - X.1361 (X.iotsec-2) (under TAP): Security framework for IoT based gateway model
    - X.1362 (2017): Simple encryption procedure for IoT
    - X.sdnsec-1: Security services using SDN
    - X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
    - X.ssp-iot: Security requirements and framework for IoT service platform
    - X.iotsec-3: Technical framework of PII handling system in IoT environment
    - X.secup-iot: Secure Software Update Procedure for IoT Devices
    - X.nb-iot: Security Requirements and Framework for Narrow Band Internet of Things
    - X.ibc-iot: Security Requirements and Framework of Using Identity-Based Cryptography Mechanism in IoT

Established March 2018

Activities related to 5G Security in SG17 (2)

- **Q7/17 (Secure application services)**
  - application/service aspects for 5G security
    - X.srfb: Security requirements and framework for big data analytics in mobile internet services

- **Q8/17 (Cloud Computing Security)**
  - Cloud computing and big data infrastructure for 5G security
    - X.sgtBD: Security guidelines of lifecycle management for telecom big data
    - X.sgBDIP: Security guidelines for big data infrastructure and platform
    - X.SRIaaS: Security requirements of public infrastructure as a service (IaaS) in cloud computing
    - X.SRNaaS: Security requirements of network as a service (NaaS) in cloud computing

- **Q11/17 (Generic technologies to support secure applications)**
  - Cryptographic profiles for 5G security
    - ITU-T X.509, public-key infrastructure
    - X.orf-gs: OID-based resolution framework for IoT group services

A newly established work item in SG17

Established March 2018

- X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems
  - To give a complete security assessment on 5G systems when commercial quantum computers are available.
  - To introduce the usage of the quantum-safe symmetric algorithms, and the quantum-safe asymmetric algorithms in 5G systems.
  - To align the security levels between quantum-safe symmetric algorithms and quantum-safe asymmetric algorithms.

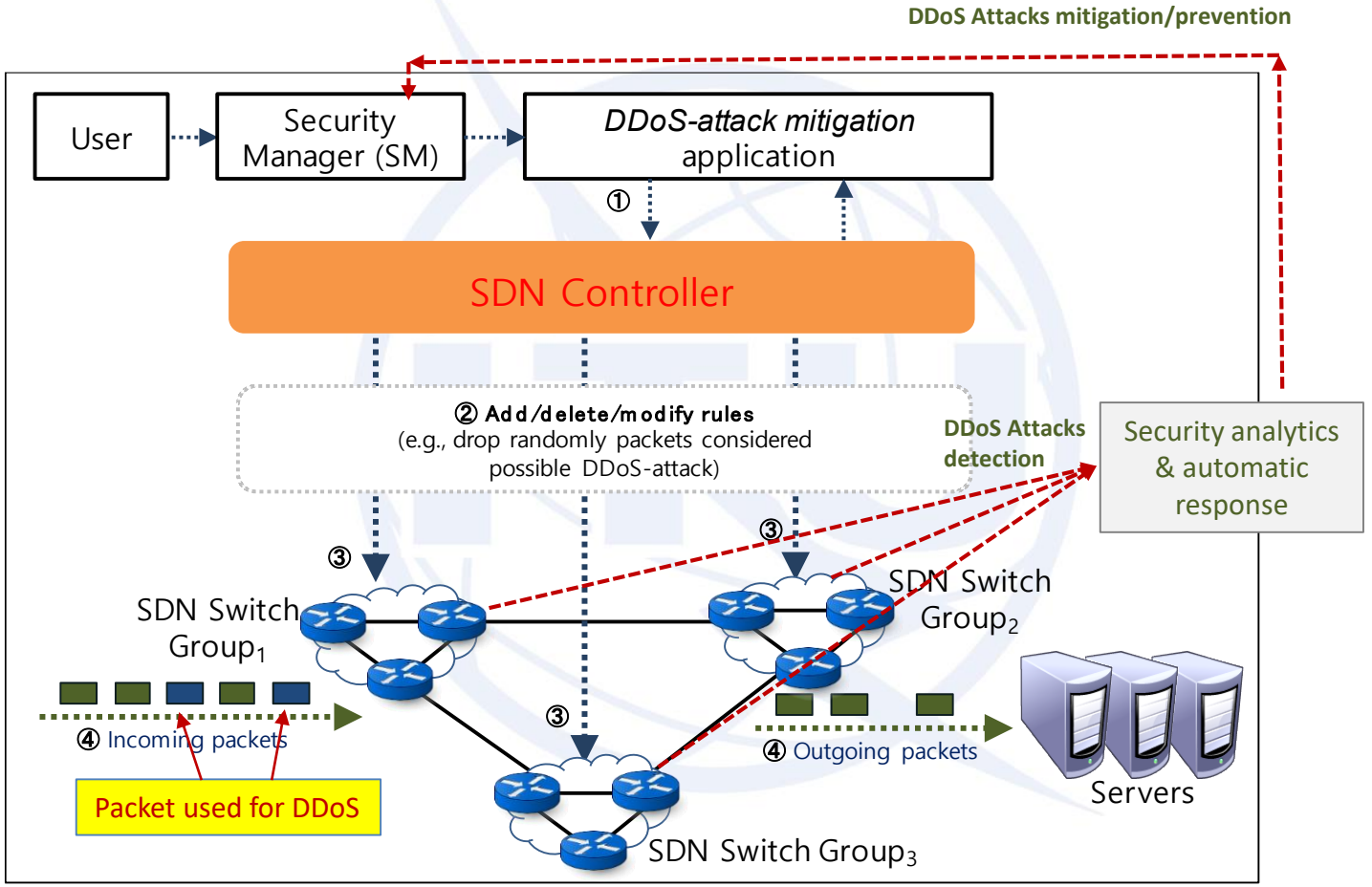
Effects on crypto-algorithms from Quantum Computers

- It is estimated that large-scale quantum computers will be available in 10 years.
- Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength, whereas many commonly used asymmetric algorithms, such as RSA, DSA and ECC, will offer no security.
- When designing 5G network, it is critical to use quantum-resistant cryptographic algorithm.

Algorithm	Key Length	Classical Bit Strength	Quantum Bit Strength	Best Quantum Attack algorithm
RSA 2048	2048bits	112 bits	0 bits	Shor's
RSA3072	3072 bits	128 bits	0 bits	Shor's
ECC 256	256 bits	128 bits	0 bits	Shor's
ECC 521	521 bits	256 bits	0 bits	Shor's
AES 128	128 bits	128 bits	64bits	Grover's
AES 256	256 bits	256 bits	128 bits	Grover's
SHA 256	256 bits	256 bits	128 bits	Grover's

(Source: Report on Post-Quantum Cryptography, NIST, April 2016)

A DDoS mitigation solution applicable to 5G, based on X.sdnsec-1



(Source: X.sdnsec-1)

Activities related to 5G Security in SG17 (3)

- **Q13/17 (Security aspects for ITS)**
  - ITS security for 5G
    - ITU-T X.1373, Secure software update capability for intelligent transportation system communication devices
    - X.itssec-2, Security guidelines for V2X communication systems
    - X.itssec-3, Security requirements for vehicle accessible external devices
    - X.itssec-4, Methodologies for intrusion detection system on in-vehicle systems
    - X.itssec-5, Security guidelines for vehicular edge computing
    - X.mdcv, security-related misbehaviour detection mechanism based on big data analysis for connected vehicles
    - X.srcd, security requirements for categorized data in V2X communication
    - X.stcv, security threats in connected vehicles

Potential work items specific to 5G security in ITU-T SG17 (1)

- Potential work items could be classified into two areas:
  - Security for implementing 5G systems
  - Security by using 5G system
- New trusted model based on security framework/architecture
- New security threats specific to 5G and their impacts
  - Threats specific to major 5G scenarios and context
  - Threats from quantum computers
- New security requirements of 5G
  - Security requirements, access control, authentication, etc. for key elements, SDN/NFV/Slicing
  - Battery-efficiency, energy-saving security mechanisms
  - Ultra reliable and low latency security mechanisms

Potential work items specific to 5G security in ITU-T SG17 (2)

- New security solutions for 5G
  - Authentication, data protection scheme
  - Global PKI, or optimization of PKI
  - Network slicing, mobile edge computing
- Security solutions using 5G systems
  - Utilize exposed 5G capabilities for security purposes
- Other security aspects of 5G system
  - Security assurance and multi-layer security certification
  - Security monitoring using AI and machine learning
  - Reference implementations or best practices

Conclusion and recommendations

- Apply built-in security (security by design) approach rather than bolt-in security one.
- Incorporate increased flexibility in security setup to meet requirement for a programmable, dynamic, and sliced 5G network.
- Make secure key components in 5G, such as SDN/NFV/network slicing, since they provide key foundation for implementing a programmable 5G network.
- Put privacy controls in place to comply with data protection regulations and contractual agreement with other organization.
- Consider a high level automation in security orchestration due to a highly dynamic 5G network .
- Adopt AI/ML based attack detection and mitigation needs to be adopted.

ITU-T SG17 welcomes feedbacks and involvement from SG13.

References

[1] ITU-T X.1038(2016), Security requirements and reference architecture for software-defined networking

[2] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov, “Overview of 5G Security Challenges and Solutions,” IEEE Communications Standards Magazine, March 2018

[3] Peter Schneider, 5G security overview, ITU workshop on 5G security, March 2018.

[4] Min Zuo, 5G Security from a Network Operator’s Point of View, , ITU workshop on 5G security, March 2018.

[5] NGMN, 5G White Paper, Feb. 2015.

[6] NISTIR 8105, Report on Post-Quantum Cryptography, April 2016

[7] ITU-T SG17 work programme, https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17

Thank you for your attention.

SAFE (Security is Absolutely First Everywhere)