Workshop summary and outcomes

22 August 2022

Heung Youl Youm
Chairman, ITU-T SG17

Session 1: Understanding the current status of 5G security and identifying improvements towards 6G

- **Moderator:** Heung Ryong Oh, ITU-T Study Group 17 Q2 Co-rapporteur | Chief Researcher, Standardization Division, TTA , South Korea
- **Presentations from:**
  - Yutaka Miyake, Director, Information and Security Department, KDDI Research, Inc.: “5G security standardization roadmap (XSTP-5Gsec-RM)”
  - Stepan Davydov, Cryptanalyst, JSRPC “Kryptonite”: “Aspects of 5G security and ways to mitigate threats”
  - Ayumu Kubota, Senior Manager, Cyber Security Laboratory, KDDI Research Inc.: “Japan’s 5G security guidelines”
  - Jonghyun Kim, WP1 Vice-Chair & Q4/17 Co-rapporteur | Principal Researcher, ETRI: “Korea’s 5G security activities”
  - Hongmei Yang, Deputy Chief Engineer, Institute of Security, CAICT: “China’s 5G security activities”

Session 1 Summary

- The published 5G security standardization roadmap by SG17 provides support in developing 5G security standards.
  - It provides an overview of 5G security from the standardization perspective, identifies opportunities for standardization through a gap analysis and provides information on both approved standards and ongoing work in relevant SDOs.
- The means to mitigate vulnerabilities related to authentication in 5G systems was also discussed.
- Finally, various 5G domestic activities were presented:
  - 5G security guidelines developed by Japan which give comprehensive guidance on securing the 5G system in practice such as technology, people and process aspects.
  - Various activities in Korea (Republic of) were presented including their 5G strategy, 5G security promotion activities and 5G/6G R&D activities.
  - China's 5G security activities in promoting 5G application and security implementation were also covered.

Session 1: Takeaways and suggestions

Takeaways and conclusions

- There is a need to identify 5G security activities at SDOs, forums, governments, etc. and provide directions for 5G-related security standardization work in ITU-T SG17.
- Controls to mitigate all vulnerabilities using the ECIES scheme and 5G-AKA protocol in 5G systems were presented .
- National initiatives for 5G security promotion covering Japan's 5G security guidelines, Korea's 5G strategy, 5G security promotion activities and 5G/6G R&D activities, and China's 5G security activities were also presented.

Suggestions to ITU-T SG17

- Continue maintaining/updating the 5G security standardization roadmap.
- Study the mitigation of all vulnerabilities related to authentication in 5G systems and explore the feasibility for this beyond 5G.
- Consider the establishment of new work items on the gaps identified such as security controls for 5G network systems.
- Develop 5G security standards considering ongoing 5G security activities at relevant SDOs, forums and governments. etc.
- Consider promoting global consensus on 5G security evaluation .

Session 2: Initial architecture and concept for 6G security

- **Moderator:** Keundug Park, Professor, AI & Blockchain Research Center, Seoul University of Foreign Studies | Q10/17 Associate Rapporteur | ITU-T JCA-IdM Co-chairman
- **Presentations:**
  - Yutaka Miyake, Director, Information and Security Department, KDDI Research, Inc.: “Brief introduction to the ITU-T FG NET-2030 and Japan’s Beyond 5G Promotion Consortium on their security-related activities”
  - Vinosh Babu James, Engineer, Senior Staff, Qualcomm India & Marja Matinmikko-Blue, Research Director, University of Oulu, Finland: “Technology trends and Scenarios for Systems beyond IMT-2020 - Initial views”
  - Anand Prasad, Partner, Deloitte Tohmatsu Cyber LLC | Former Chairman of 3GPP SA3: “Path to beyond 5G Security”
  - Junzhi Yan, Senior researcher, China Mobile Research Institute: “How to utilise PQC for 6G security“
  - Jeong Min Lee, Manager, AI BIGDATA Team, Korea Internet and Security Agency (KISA): "Cybersecurity AI Dataset in 6G Era"
  - Jonghyun Kim, WP1 Vice-Chair & Q4/17 Co-rapporteur | Principal Researcher, ETRI: “Korea’s research status on 6G security”

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Security topics related to 5G/B5G/6G are based on new technologies, new mechanisms, new use cases, etc.
- Work has started in WP5D towards the evolution of IMT systems beyond 2020
  - Timeline for IMT evolution into 2030 and beyond is now available
  - Report on future technology trends reached DNR stage
  - Recommendation of IMT vision is ongoing
- Normative work yet to start in standards and industry bodies

Suggestions to ITU-T SG17

- Identify security standardization topics from ongoing 5G and B5G activities.
- Enhanced coordination and collaboration amongst the different ITU organs and external organizations is encouraged from the beginning.
- Solicit input, from the security point of view, to vision document for the IMT 2030 to ITU-R WP5D.

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Cybersecurity AI datasets are effective within the region, but international cooperation is still difficult
- Korea's 6G R&D strategy as well as ETRI's work and global collaboration project on 6G security were introduced in detail

Suggestions to ITU-T SG17

- Consider the feasibility of standardization of frameworks and schema for cybersecurity AI datasets.
- Consider the feasibility of security standardization for 5G and beyond including topics such as the feasibility of autonomous security frameworks and requirements for security-by-design (native security).

Session 3: Fundamental security requirements and functions for 6G

- **Moderator:** Kyeong Hee Oh, Q14/17 Co-rapporteur
- **Presentations:**
  - Gyu Myoung Lee of Liverpool John Moores University (LJMU) explained about general aspects of future networks including trust networking
  - Ke Wang from China Mobile Research Institute explained security concepts for 5G and beyond
  - Fanqin Zhou of ITU-T Study Group 2 introduced SG2 work on security management and user IAM for TMN
  - Mika Ylianttila of University of Oulu detailed fundamental specified 6G security requirements.
  - Xiongwei Jia from China Unicom introduced computational issues for access networks

Session 3: Takeaways and suggestions

Takeaways and conclusions

- 6G will merge different types of networks, new types of technologies such as AI, IoT, DLT, VR, etc. and new management technologies.
- The convergence of technologies will put new requirements for security and privacy to establish trust in the network. The future network will be trust-native and security is a core part of it.
- The evolution of technologies also affects telecommunications management networks, like how to manage multiple operators' cooperation securely and effectively.

Suggestions to ITU-T SG17

- Prepare for future standardization by collaborating with other SDOs and SGs such as SG2, SG13, SG 20, etc., to provide security with the introduction of new technologies for 5G and beyond.
- Continue to develop technical standards on security to build confidence in the use of ICTs in evolving future networks.

Session 3: Takeaways and suggestions

Suggestions to ITU-T SG17

- Further topics for consideration of special session of follow-up of ITU workshop on security for 5G and beyond at August/September 2022 SG17 meeting:
  - Systematized built-in security to form an immune ability against internal attacks
  - Enhanced security design e.g., wireless physical layer security
  - AI bring intelligence to security
  - DTN bring certainty to security intelligence
  - From passive protection to active perception
  - Secure interoperability of heterogeneous network(air-space ground) convergence
  - Coordination of computing and network security
  - End, edge, network and cloud security capabilities collaboration
  - Dynamic and flexible security capability deployed on demand
  - Integrated response and recovery capabilities to improve network resilience

Session 4: Panel discussion – Collaboration and coordination on IMT-2020 and beyond security standardization activities

- **Moderator:** Koji Nakao, NICT, Japan | WP3/17 Chairman
- **Panelists:**
  - Zhili Wang, PhD, Associate Professor, BUPT, China | ITU-T Study Group 2
  - Zhiyuan Hu, Director, Security Research, Vivo Mobile Communication Co. Ltd.: “Status in SG17”
  - Christopher Mulley, Principal Architect, ZTE, China
  - Anand Prasad, Partner, Deloitte Tohmatsu Cyber LLC | Former Chairman of 3GPP SA3
  - Suresh Nair, Security Standards Specialist, Nokia Bell Labs | Chair, 3GPP Security WG SA3
- **Questions to panelists:**
  - *Technology-related:* What security technologies do you see essential/critical in the 6G era? | What is your perception of the threat landscape in the 6G era?
  - *Standardization-related:* What should be the standardization direction? | What kind of issues should be standardized in SG17 for 6G?

Processes for security consideration on 6G

- Based on presentations from the previous sessions, the following processes were identified as requirements when developing and considering 6G security:

1. Vision/Concept of 6G including use cases
2. High level 6G requirements
3. High level 6G security requirements
4. Possible 6G basic system construction → 6G specification
5. Threats assessment for identifying 6G threats
6. More specific security requirements
7. Possible security controls

ITU-R, FG NET-2030, etc (supported by SG17)

3GPP

SG 17

Standardization related to SG17

A) Recommendations for: network carriers, service providers, service users

B) Content to be standardized in SG17:

Security capabilities for:

- Technologies – including “mechanisms”
- Personal
- Physical
- Management

C) Topics for specific consideration:

- Trust, PQC, AI, Adaptive security, Flexible security, ….

Session 4: Takeaways and suggestions

Takeaways and conclusions

- When considering 6G security, it is important to clarify the 6G vision and initial concepts. SG17 should stay updated on the developing status of 6G and provide possible security advice.
- In proceeding with the study of 6G security, it will be necessary to collaborate with ITU-R, 3GPP and other relevant groups on the vision/concept for 6G. In particular, strong collaboration with 3GPP on 6G specifications will be important to SG17 in identifying 6G security technologies.
- It is important for SG17 to clarify security functions (capabilities) for 6G security. Identified security functions should be studied in-depth in SG17.
- Security technologies identified in the session for SG17's focus are listed on the next slide.

Suggestions to ITU-T SG17

- Continue collaboration and cooperation with relevant groups such as SG2, SG13, 3GPP SA3, ETSI, CEN, and ITU-R WP5D.
- Support other groups to develop the security vision/concept for IMT2030.
- Support more specific security requirements for 5G and beyond.
- In coordination with experts from 3GPP SA3 and other relevant groups, identify specific security technologies for 5G and beyond.

Security technologies

- The following technologies were identified for SG17's focus from session 4:
  - Network management system – access control
  - Accessibility
  - Zero trust
  - AI security
  - Autonomous security – patch management
  - Physical security
  - DLT security
  - End-to-end federation
  - Identity management – including biometrics
  - Mobile communication system – authentication mechanisms, key management,
  - PQC – how to utilize the PQC…
  - Adapting evolution of 6G technologies
  - Sustainability should be considered for 6G security.

Thank you for your attention.