Way forward to SG17 for session 4

ITU Workshop on Generative AI: Challenges and Opportunities for Security and Privacy, 20 February 2024, Geneva

Heung Youl Youm, PhD/Mr.
ITU-T SG17 Chairman
Soonchunhyang University, Korea (Republic of)

SOON CHUN HYANG UNIVERSITY

Need to increase coordination role of SG17 across SDOs in this study area, consequence of generative AI

- ITU, specialized agency under the United Nation and security competence center:
  - SG17, providing international standards to build confidence and security in the use of ICTs.

ISO

- ISO/IEC TS 5723:2022 - Trustworthiness — Vocabulary

IEEE Networking the World™

- Enabling End-User Agency and Trust in Artificial Intelligence Systems

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

- ISO/IEC CD 27090 - Cybersecurity — Artificial Intelligence
- ISO/IEC 27091 AI privacy

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
OECD

- Tools for trustworthy AI:

ITU

Current work items and SG17 agreement

- Current work items under development
  - X.sr-ai, Security requirements for AI systems, established on Aug/Sep 2023 SG17 meeting
  - XSTR-SEC-AI - Guidelines for security management of using artificial intelligence technology, agreed on August/September2023 SG17 meeting
  - Two new work item proposals for this meeting including “Proposal for new work item X.sgGenAI: Security Guidelines for Generative Artificial Intelligence Application Service ”.

- SG17 agreements as of now
  - The March 2023 SG17 meeting and CG meeting during May – July 2023 agreed on:
    - “consequence of Generative AI” together with other 15 topics considered as emerging topics for the next study period(2025-2028)
    - Plan to consequence of generative AI to be incorporated by Q7/17, to be confirmed.

Other SDOs and recommendations to SG17

- Other SDOs for collaboration
  - ISO/IEC JTC 1/SC 27/WG 4 security and WG5 for privacy, ISO/IEC JTC 1/SC 42/WG 3 for Trustworthiness.
  - Other groups such as ITU-T SG13 for AI/ML, IEEE for Trust and Agency, OECD for trustworthy AI, other groups.

- Recommendations
  - Need to identify gap to proceed with new work items.
  - Study complete aspects for security, PII protection and trustworthiness for generative AI.
  - Undertake studying consequence of generative AI as well as controls to mitigate the negative consequence of generative AI.
  - Promote coordination activities, for example, by using a joint coordination group inviting relevant SDOs with the objectives to avoid duplicative work as much as possible and diversity of standards among SDOs.
  - Study the positive aspects of using generative AI to identify opportunities in terms of security and trustworthiness
  - Consider the requirements from regional or national regulations and ethics.

Thanks!