AI/ML and Security standardization

Zhaoji Lin

WP4 co-chair

Security of AI/ML-enabled network and service

- Security for AI in 5G
  - Introduce new NF in 5GC (NWDAF)
  - RAN-centric Data collection and Utilization
- Security for ENI(Experiential Networked intelligence)
  - As ENI exposes new interfaces, APIs and Reference Points, which optionally expose new attack profiles, ENI will provide mitigation against attacks focusing on those new attack profiles
- Security for ZSM (zero-touch network and service management)
  - Data privacy, integrity, confidentiality; security policies automatically application; automated attack detection, identification, prevention, and mitigation

Security for the main building blocks of AI/ML

- **Computation power /infrastructure security** (cloudification security, edge-cloud coordination security, security transparency and trustworthy)
- **Mass-collected data security** (data privacy, data lifecycle management, de-identification, reverse attack)
- **Algorithm security** (risk evaluations, assurance methodology, anti – bias & discrimination, algorithm blackbox)

Security application empowered by AI/ML

- Unknown threats detection with AI
- Fraud detection with AI
- AI enabled IDS/IPS
- AI based network Security situational awareness
- AI based content filtering
- ……

Standardization Gap analysis

- **NIST:** develop a broad spectrum of standards for AI data, performance, interoperability, usability, security and privacy, in order to cultivating Trust in AI Technologies; to measure and enhance the security and trustworthiness of AI systems
- **ISO/IEC JTC 1/SC 42:** AI trustworthiness, governance…
- **ETSI ISG ENI:** network assurance (network fault identification and prediction, assurance of service requirements); security for exposed new attack profiles (ENI assisting MANO, MEF LSO)
- **ETSI ISG ZSM:** security requirements when introduce ZSM RA to 5G network
- **3GPP :** RAN-centric Data collection and utilization for NR and LTE(FS_LTE_NR_data_collect)/enablers for network automation for 5G(FS_eNA). Security has not yet been taken into account.

SG17’s way forward in studying AI/ML security

- Prefer a distributed approach among multiple Questions to a centralized approach by a single Question, as AI is a combination of multiple technologies
  - AI-based Security application – Q4,Q5,Q7
  - data security for AI – Q3,Q8
  - security for AI infrastructure– Q2,Q6,Q8,Q10,Q11

Thank you!