All Sessions Outcome

ITU Workshop on Artificial Intelligence, Machine Learning and Security

Geneva, Switzerland, 21 January, 2019

Session 1: Using AI and ML technologies for security – part 1

Takeaways and Conclusions

1. Machine learning techniques can improve efficiency of APT defense, particularly in areas like DGA (domain generating algorithm) and unknown malware detection.
2. AI empowered cyber defense can have capabilities to analyze and understand security situations and automate security operations within an organization.
3. Study customer privacy enhancement by using machine learning technology.
4. Study overall cyber threats for telecom network and how does AI mitigate the cyber threats.
5. Analyze key challenges and solutions when introducing AI to cybersecurity.

Suggestions to SG17

- ❑ To kick off new work item in SG17 on unknown threat defense by utilizing AI/ML technology.
- ❑ To consider standardization of security metrics on AI/ML-based security situation awareness and security operation automation.
- ❑ To identify new privacy enhancement schemes for anti-spam by using machine learning technology.
- ❑ To identify cyber threats that telecom network is facing and utilizing AI to mitigate them from architectural and technical perspective, like signaling anomaly detection, radio resource attack detection, dataflow based IoT threat detection, internal network anomalies detection, automated configuration management.
- ❑ Definitely, we need standardization for AI for security, however, it will evolve with the progress of AI technologies.

Session 2: Security threats and privacy risks of AI and ML applications

Takeaways and Conclusions

1. How to deal with ”machine bias”?
2. Transparency and Trustworthiness are two fundamental aspects requiring further definition and development.
3. Unbalanced stakeholder representations:
    1. Too Much on Developers
    2. Not enough on Human users
4. AI/ML technologies should be utilized in the context of the bigger life cycles and inline with risk management.
5. “Knowledge” seems to be the ‘big forgotten’ in the landscape and echoes the ‘syntax/semantics’ debate. Investing here should reinforce the understanding of models and help supporting Transparency and Trustworthiness.
6. AI/ML in the real example of online Fraud gives many lessons learnt and wins over traditional anti Fraud measures
    1. User Activity is hard to mimic by attackers and so is a good source of information;
    2. Combining various AI/ML algorithms improves results

Suggestions to ITU-T SG17

- □ To develop terminology and ontologies for the ICT (and OTTs) including:
    - □ Levels of autonomy, analogous to the levels 1-5 for self driving car
    - □ Levels or impact of decisions
    - □ Levels of privacy preservation
    - □ Taxonomy for the type of AI/ML employed
    - □ Durability, versioning and/or persistence of a model
    - □ Taxonomy of security use cases addressed by a solution
    - □ For classifier systems: formats for train / test and efficacy comparison
    - □ Transparency evaluation guidelines (Data, Business/Management model, Technical framework)
- □ To encourage the development of research in Stakeholder representations, Knowledge vs Models, Transparency/Interpretability/Trustworthiness and the Human Being in this loop.
- □ There is scope for standardization by ITU-T SG17.

Session 3: Using AI and ML technologies for security – part 2

Takeaways and Conclusions

1. ML needs a new process and experts to apply.
2. AI with autonomous driving can detect fraud in fin-tech systems precisely.
3. AI technologies can secure 5G systems including eMBB (enhanced Mobile Broad Band), mMTC (massive Machine Type Communications), URLLC (Ultra Reliability and Low Latency Communications), MEC (Multi-Access Edge Computing), Network Slicing, etc.
4. Although the expansion of cellular area using drones is attractive, this may introduce vulnerabilities, such as easy accessible network nodes, hacked drones, various network backdoors, etc.
5. Trustworthiness of AI is one of big issue in security area.

Suggestions to ITU-T SG17

- ❑ To study guidelines for applying ML technologies that will be required from the perspective of users.
- ❑ To study AI technologies that can be applicable to fin-tech security.
- ❑ To work on AI technologies that can be applicable to 5G systems and applications to improve security.
- ❑ To develop new functions using AI technologies that may introduce vulnerabilities, so security is also considered to standardized such new functions.
- ❑ Collaborate with SC42 on trustworthiness of AI, if required.

Session 4: Panel discussion – Future directions on cybersecurity standardization activity

Takeaways and Conclusions

1. Identified security subjects categorized into three areas:
   security by AI, security of AI, security from AI(risks from AI).
2. Study an AI-based fraud detection to support operators.
3. Start first with terminology and ontology related to AI security.
4. Keep harmonization and minimize duplication and with other SGs and SDOs such as ISO/IEC JTC 1/SC 42.

Suggestions to ITU-T SG17

- ❑ To develop a SG17 standardization roadmap for AI security through the gap analysis.
- ❑ To choose distributed approach by multiple Questions in SG17:
  - ❑ AI security has the broad scope that would be studied by multiple Questions in SG17, especially Q2/17 for the security framework for AI.
- ❑ Cooperate with other ITU-T study groups and external groups, such as ISO/IEC JTC1/SC42, IEEE and 3GPP.