AI/ML security in mobile telecommunication networks

ENISA Telecom & Digital Infrastructure Security Forum 2024

Patrik Teppo, Senior Expert Security Architecture 2024-05-15

Agenda

AI/ML technology from telecom security perspective

AI/ML as tools employed by threat actors to attack networks

AI/ML as tools to enhance network security

AI/ML components integrated in networks

Securing AI/ML components in networks

- AI/ML threat landscape in mobile telecommunication networks
- AI/ML threat mitigation in mobile telecommunication networks

Holistic security approach based on Ericsson trust stack

AI/ML technology from telecom security perspective

AI/ML as a tool for threat actors to attack mobile telecommunication networks

AI/ML as a tool to enhance security of mobile telecommunication networks

AI/ML technologies integrated into mobile telecommunication networks as targets for attackers and how to protect them

AI/ML as tools to attack telecom networks

- Stakeholders must consider impact of offensive AI/ML on cybersecurity risks
  - AI/ML can substantially change both type and scale of these risks

- AI/ML amplifies effectiveness and reach of existing attacks
  - Enhance attack automation by enabling adversaries to find vulnerabilities and exploit them
  - Identify most vulnerable or valuable targets within telecom network by analyzing vast datasets
  - Adapt attacks in more responsive and intelligent manner in real-time
  - Using AI models to convey malicious content
  - Repurposing available AI tools, especially LLM-based with malicious intent

AI/ML opens new frontiers in cybersecurity defense

- AI/ML enhance threat detection by supporting traditional methods and identifying new threats
  - AI-based security controls can employ advanced behavioral analysis and real-time adaptation, helping match evolution of attacker techniques
- Automate and enhance security assurance practices
- Reduce human induced risks through automation

Offensive AI requires advanced countermeasures

Specialized AI-powered security controls, e.g., AI-driven IDS, designed to detect AI-driven attacks

Real-time adaptation is important against AI-based attacks, which can adapt themselves faster than humans can react

Securing AI/ML components in telecom networks

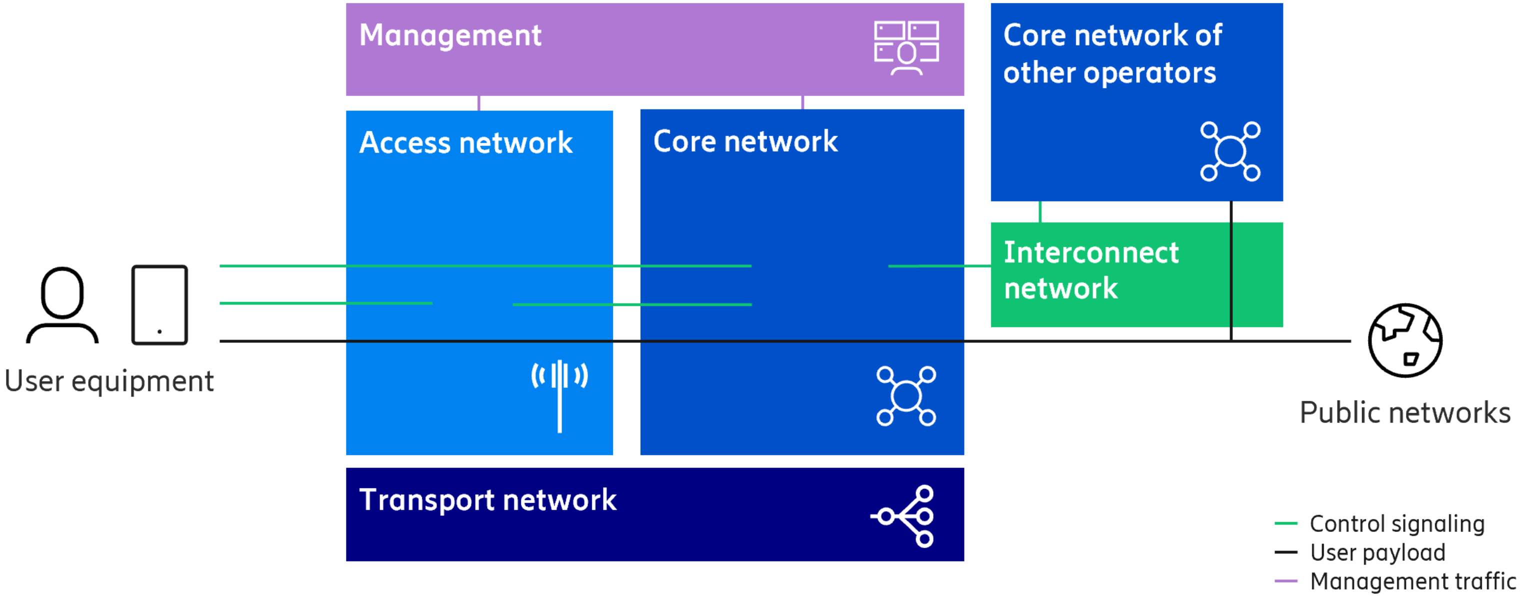
AI/ML adds **capabilities and efficiencies** in mobile telecommunication domain, analyzing security and trustworthiness is vital as AI/ML may introduce new security risks

Integrity of AI/ML models and data they process is important, compromise can result in service disruptions to breaches of sensitive user information

AI/ML components integrated into mobile telecommunication networks are not invulnerable

AI/ML components within telecom

- 5G RAN or 3GPP NG-RAN
- RAN based on O-RAN architecture
- Network Data Analytics Function (NWDAF) within 5G core network
- AI-driven Operations/Business Support Systems (OSS/BSS)
- Security management tools



Integration of AI/ML to 5G system without appropriate security measures may elevate security risks in mobile telecommunication networks

AI/ML environment threats

- AI/ML environment threats target vulnerabilities in components surrounding AI/ML
  - Execution environment, data storage, etc.
- Traditional forms of attacks
  - Not designed to exploit AI/ML vulnerabilities, but can compromise AI/ML system
- Target software development life cycle, deployment procedures, or communications
  - Result in compromised components or new exploitable vulnerabilities

Threats relevant to AI/ML environment include:

Unauthorized access to training data or model itself

Disruption of operational environment, including DoS attacks

Supply chain attacks targeting critical components like ML software stack, or hardware elements

AI/ML specific threats

- Assets at risk include AI/ML models and relevant data integrated into telecommunication system
- Attackers aim to compromise or manipulate these for various purposes, including disrupting operations or stealing IP

AI/ML-specific threats according to NIST taxonomy

Evasion attacks aim to alter ML model behavior with crafted queries, or prompt injection attacks on LLM models

Poisoning attacks contaminate training data or parameters, establishing backdoors and impacting deployment outcomes

Privacy (data disclosure) attacks aim to extract information about the training data, targeting data or ML model

AI/ML threat mitigation in telecom networks

Identify threats to AI/ML environment and AI/ML assets by performing security risk assessment

Mitigate identified threats, at first, implementing traditional security and privacy controls

Traditional security effective against environment threats and address some AI/ML-specific threats:

- Ensure confidentiality, integrity, availability, and authenticity; only authorized access to data and ML models; verify data and model sources
- Security monitoring, auditing, and accountability practices detect anomalies and ensure compliance with security standards
- Data and model retention policies define storage durations and conditions for deletion or archiving
- Continual security training is necessary to understand and uphold AI/ML system security

Specialized security for AI/ML systems

Techniques for detecting and preventing AI/ML-specific attacks are outlined in NIST AML or OWASP

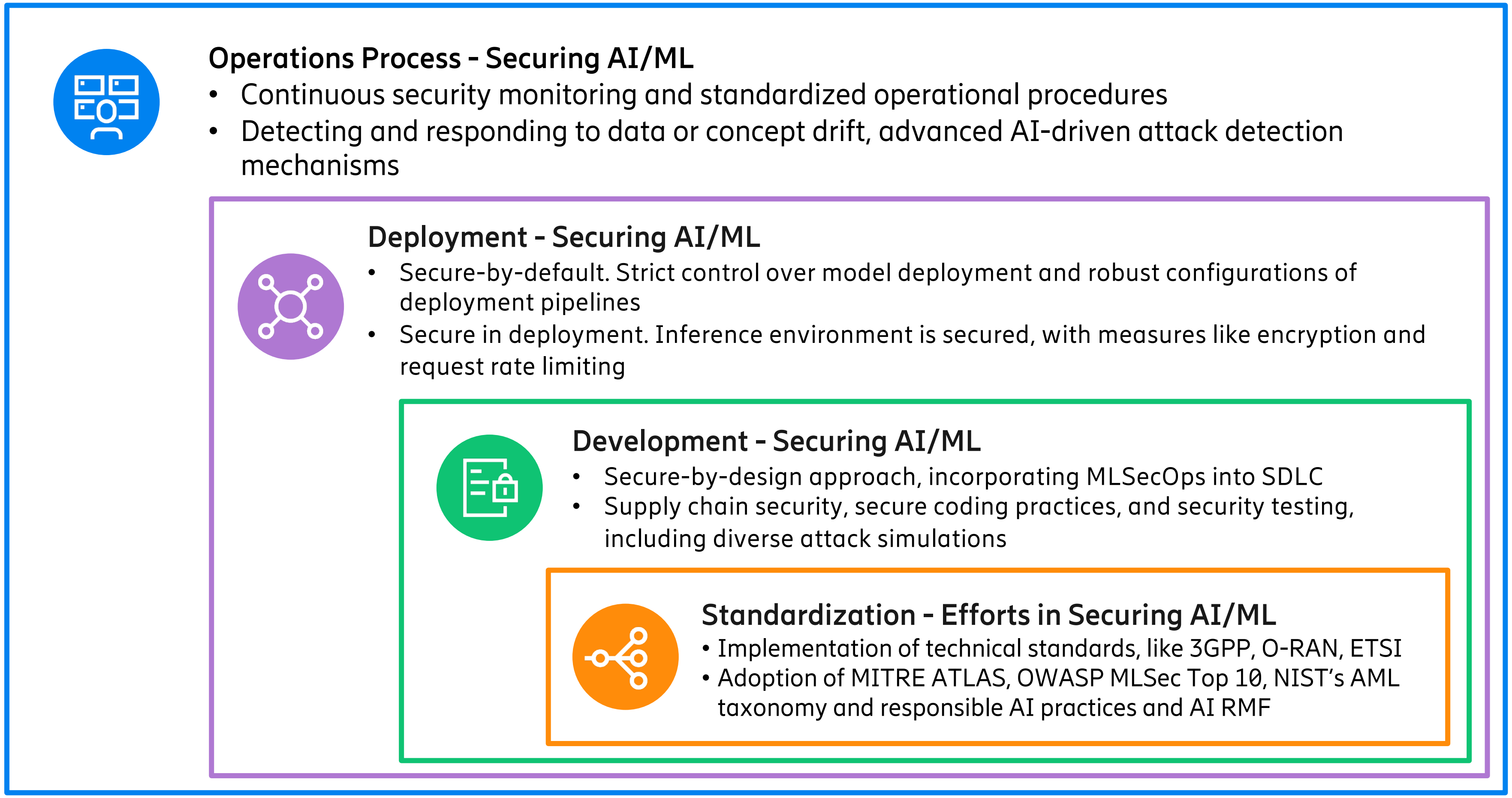
AI/ML attacks and mitigations are subject to ongoing research, suitability of these methods requires further investigation and should be tailored to specific use cases. Good practices to consider include:

- Resilient model design
- Model explainability, transparency, reproducibility, and auditability
- Evasion attacks mitigation: robustness against evasion samples, adversarial sample detection, etc.
- Poisoning attacks mitigation: training data sanitization, training data distribution monitoring, etc.
- Privacy attacks mitigation: model extraction detection, Privacy-Enhancing Technologies (PETs), etc.

AI/ML-specific vulnerability analysis focuses on unique risks inherent to ML models and their data

- Complexity of such analysis comes from the non-deterministic nature of AI/ML systems and the evolving nature of models, which complicates assessment of test results

Securing AI/ML using Ericsson Trust Stack



Operations Process - Securing AI/ML

- Continuous security monitoring and standardized operational procedures
- Detecting and responding to data or concept drift, advanced AI-driven attack detection mechanisms

Deployment - Securing AI/ML

- Secure-by-default. Strict control over model deployment and robust configurations of deployment pipelines
- Secure in deployment. Inference environment is secured, with measures like encryption and request rate limiting

Development - Securing AI/ML

- Secure-by-design approach, incorporating MLSecOps into SDLC
- Supply chain security, secure coding practices, and security testing, including diverse attack simulations

Standardization - Efforts in Securing AI/ML

- Implementation of technical standards, like 3GPP, O-RAN, ETSI
- Adoption of MITRE ATLAS, OWASP MLSec Top 10, NIST's AML taxonomy and responsible AI practices and AI RMF

- End users' experience of network security is determined by deployed networks
- Security status of deployed networks depends on four inter dependent levels
- Holistic approach to security includes all four levels
- Operators are in control of operations, deployment and integrator and vendor selection
- Vendors are in control of their product development and sourcing decisions (component suppliers)
- Standards are set in a multi stakeholder fashion

What about AI/ML in telecom network security - Ericsson