Building trustworthiness in future mobile networks

Eva Fogelström
Director Security, Ericsson Research
5G
Non-limiting access to information and sharing of data for anyone and anything
Beyond 5G

- Trustworthiness of systems
- Sustainability
- Automatization and digitalization
- Limitless connectivity
Technology journeys – sample stepping stones

- Next-gen devices, sensing & actuation
- Interoperability
- Distributed ubiquitous sensors & actuators
- Interoperability
- Network as a mediator for intelligent machines
- Network platform enablers for the Internet of senses
- The Internet of senses
- Digital twins & Cyber-Physical Systems everywhere
- Ubiquitous fully autonomous Systems of Systems
- Digital infrastructure for the programmable world
- Merged virtual & real worlds
- Extreme performance
- Limitless connectivity
- Trustworthy systems
- Cognitive network
- Network compute fabric
- Network as a mediator for intelligent machines
- Digitalized & programmable physical world
- Connected intelligent machines
- Connected sustainable world
- Digital infrastructure for the programmable world
- ICT for sustainable, resilient societies
- ICT for climate & dematerialization
- Resource-efficient ICT
- Network adaptability
- Secure IDs & protocols
- AI agents for network functions
- Cloud-native network development
- Solutions built on confidential computing
- Support for zero-energy & -cost devices
- E2E security assurance across the lifecycle
- Autonomous system operation
- Network platform enablers for the Internet of senses
- Digital infrastructure for the programmable world
- Merged virtual & real worlds
- Extreme performance
- Limitless connectivity
- Trustworthy systems
- Cognitive network
- Network compute fabric
Special attention: security and trust

- Mobile networks part of critical infrastructure
- Special attention to reliability, resilience, availability, security, privacy, safety, and assurance
- Ongoing initiatives focusing on security and trustworthiness of mobile networks

- EU toolbox for 5G security
- ENISA threat landscape for 5G
- NCSC security analysis for the telecom sector
- NIST efforts on trustworthy information systems
- IIC work on trustworthiness for IoT
- Security assurance in 3GPP and GSMA
- ...

Fundamental question: How do we know that we can trust the networks to perform as expected when facing new use cases, new requirements, and new types of attacks?
Trust is a firm belief

Trustworthiness comes from evidence
Where is security in 5G?

5G security

confidentiality
integrity
availability

Ecosystems

Standards

Products

Deployment

Operations Maintenance

2G

User equipment
(mobile station in 2G)

3G

Access network

Core network
(visited)

4G

GSM AKA

GPRS AKA

Identity confidentiality
by TMSI/P-TMSI

Identity confidentiality
by TMSI/P-TMSI

5G

User equipment
(mobile station in 2G)

Identity confidentiality
by SUCI

Eva Fogelström  |  2020-11-12  |  Ericsson
5G standardization

5G security

- Trustworthiness
  - Resilience
  - Communication security
  - Identity management
  - Privacy

- Resilience in radio and core
- Devices and network infrastructure
- Strong and flexible
- Trusted network equipment
- Enhanced by design

Eva Fogelström  |  2020-11-12  |  Ericsson
Building trustworthy mobile networks

Three key technology areas

Diligence in enabling a trustworthy architecture

Secure supply chain and CI/CD process

Deployment and (re)configuration

Identify, detect
Respond

Deployed system capabilities

Assurance and defense: AI as a powerful tool

Network reliability, availability, and resilience

Trust foundations: confidential computing and secure identities

System trustworthiness

System management capabilities

Threat and risk landscape

Eva Fogelström | 2020-11-12 | Ericsson
Confidential computing

- Confidential computing and secure identities for provable security in cloud and edge compute, and for connected things and industries
- Secure enclaves within processor hardware (trusted execution environment) – root-of-trust
- Remote attestation: key tool in assessing the trustworthiness of a service, assuring execution on intended hardware
Virtualization and root of trust

- Service-based architecture for 5G core networks uses virtual network functions built from microservices in containers
- Service orchestration: networked functions automatically placed on state-of-the-art cloud computing platforms utilizing security functions integrated within processor hardware
- Hardware-based root-of-trust for assurance
- Remote attestation can securely bootstrap containers and virtual machines for virtual network functions in the infrastructure
Secure identities

- Identities are essential for secure communication in mobile networks: device-to-network, node-to-node, node-to-server
- SIM to securely store identities and keys for authentication to mobile network
- eSIM for IoT allows to bootstrap and assume localized profile
- Interest for iSIM implemented in trusted environment within system-on-chip
- Anchor trust for identities to specific functionality in networks, anchor trust in network to hardware-based root
Trust chain

- Identity used in one layer may serve as root-of-trust to derive identities in other layers
- Example authentication and key management for applications (AKMA) in 5G: identity in SIM is used for security on application layer
- For IoT applications and eMBB
Security assurance

- Requirements and auditing for security assurance, e.g. NESAS
- Need mechanisms for monitoring and compliance verification of mobile networks, including virtualized network functions with highly dynamic behavior
- AI to analyze and understand large network systems to determine the level of compliance with different security requirements and policies
- AI powerful tool to detect or predict compliance failures, to facilitate investigation of incidents, locate root cause, to make recommendations
AI for network security

- AI powerful tool to strengthen mobile network security during operations
- Threat intelligence
- Attack detection and response
- Network-based monitoring of devices to detect deviations and respond to malicious or faulty behavior
- Automated security management
- Detection of false base stations through existing mechanisms for measurements data collection
Security for AI

- Privacy concerns and a need to protect models and algorithms
- Cryptographic techniques to secure AI and protect information
- Confidential computing to protect algorithms and underlying models, and to address privacy needs in multi-tenant environments
- Adversarial attacks
- Explainable AI
Responsible AI

- Trustworthy AI, responsible AI, AI ethics: balance between positive effects and potential misuse of information and communication technology
- Adoption of ethical principles to build trustworthy systems
- European Commission’s ethics guidelines for trustworthy AI: technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, accountability
- Explainability of AI models and results
Towards the future

• Reliability, availability, resilience + adaptability, explainability, transparency to meet demands on security and trustworthiness of virtualized network functions, connected intelligent machines, limitless connectivity, in a digitalized and programmable world

• Part of the journey:
  • Confidential computing and security identities
  • Security assurance, verification, formal proof
  • Software and hardware security
  • AI security, explainable AI, protection of data and models
  • Security, privacy, safety in development, deployment, and operations