Safety and security traps of 5G for PPDR

Marko Pust, 5G Safety Workshop

Bled, 14.12.2018

Naložbo financira Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

Agenda

- About us
- Cybersecurity, and why it concern us
- Tradional approach to security
- Specifics of 5G security
- Proposed framework
- Questions and discusion

About us

- IT infrastructure
  - Mission critical systems
- PKI infrastructure
- Security services
  - Data security
  - Security management
  - Identity management
- Custom development
  - Java

The „old“ and the „new“ way

Threat actors

- Organized crime
- Hactivist groups
- Insiders
- Nation state.

Traditional security practice

- User identity management based on (U)SIM
- Mutual authentication between network and users
- Securing the path between communication parties.

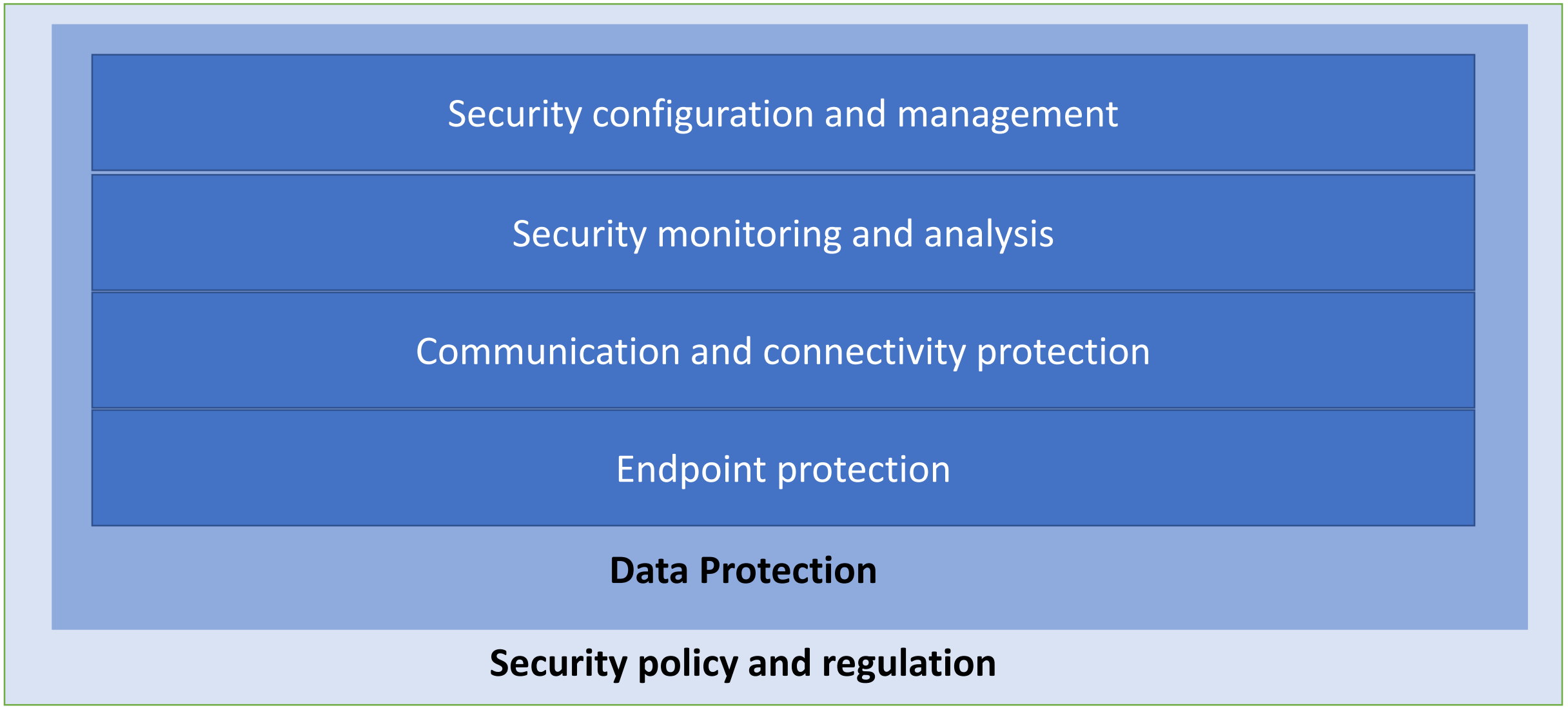
Security challenges ahead of 5G

- New business models.
  - Diversity of applications and services
  - PPDR, IoT, …
- IT-driven network architecture
  - SDN
- Heterogeneous access
  - One of the features of next-generation access networks
  - Different access technologies (WiFi, LTE…)
  - Security architecture suitable for different access technologies.
- Privacy protection
  - Healthcare, smart home, smart transport…
  - Privacy leak can cause a serious consequences.

What is the remedy?

- 5G in mission critical application will bring a new focus to security chalanges.
  - … but basic concepts still remeinst the same.
- Embedded security into all phases of the lifecycle
  - Security (and privacy) by design
- Several IT security methodologies

Security framework functional building blocks



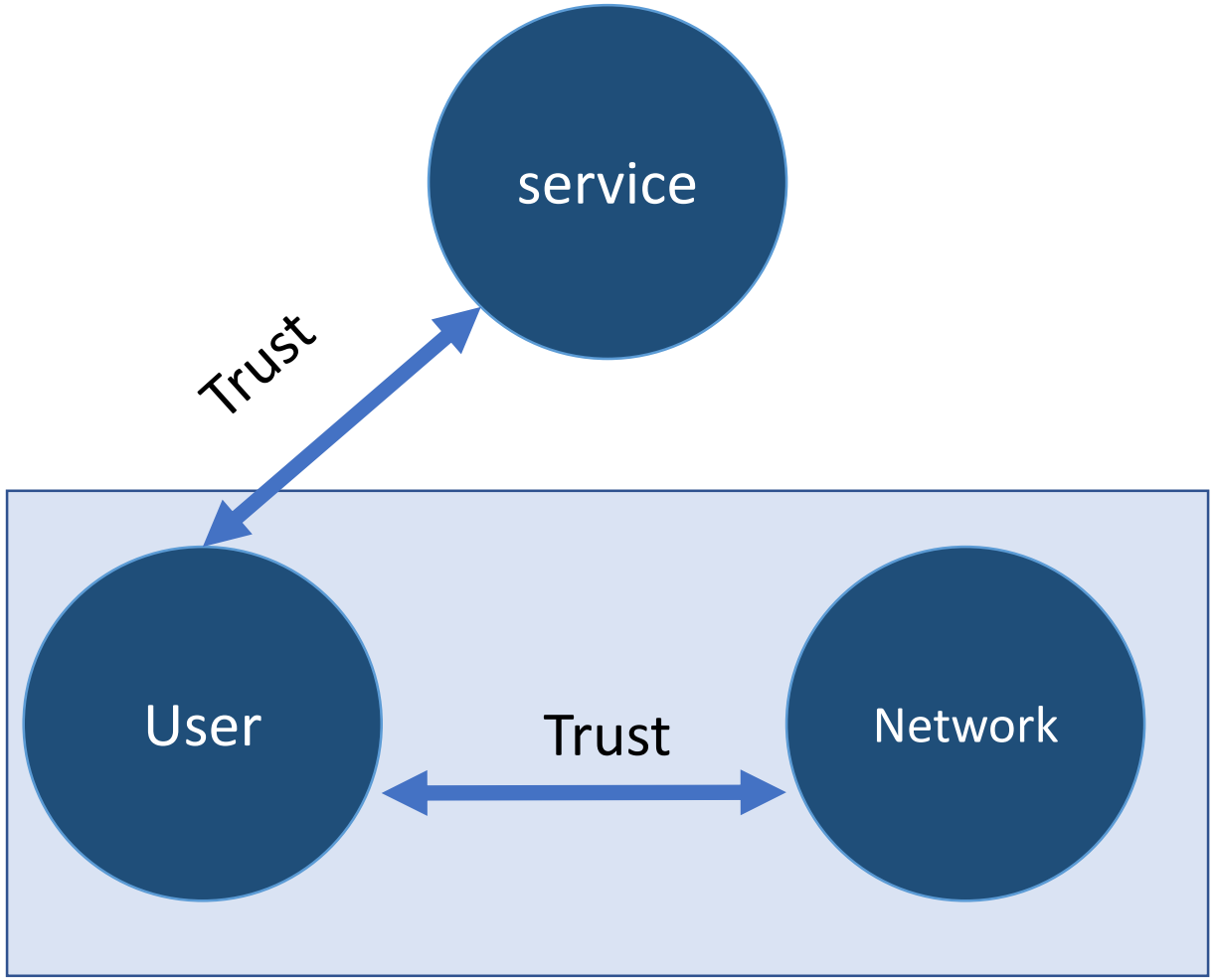
Endpoint protection

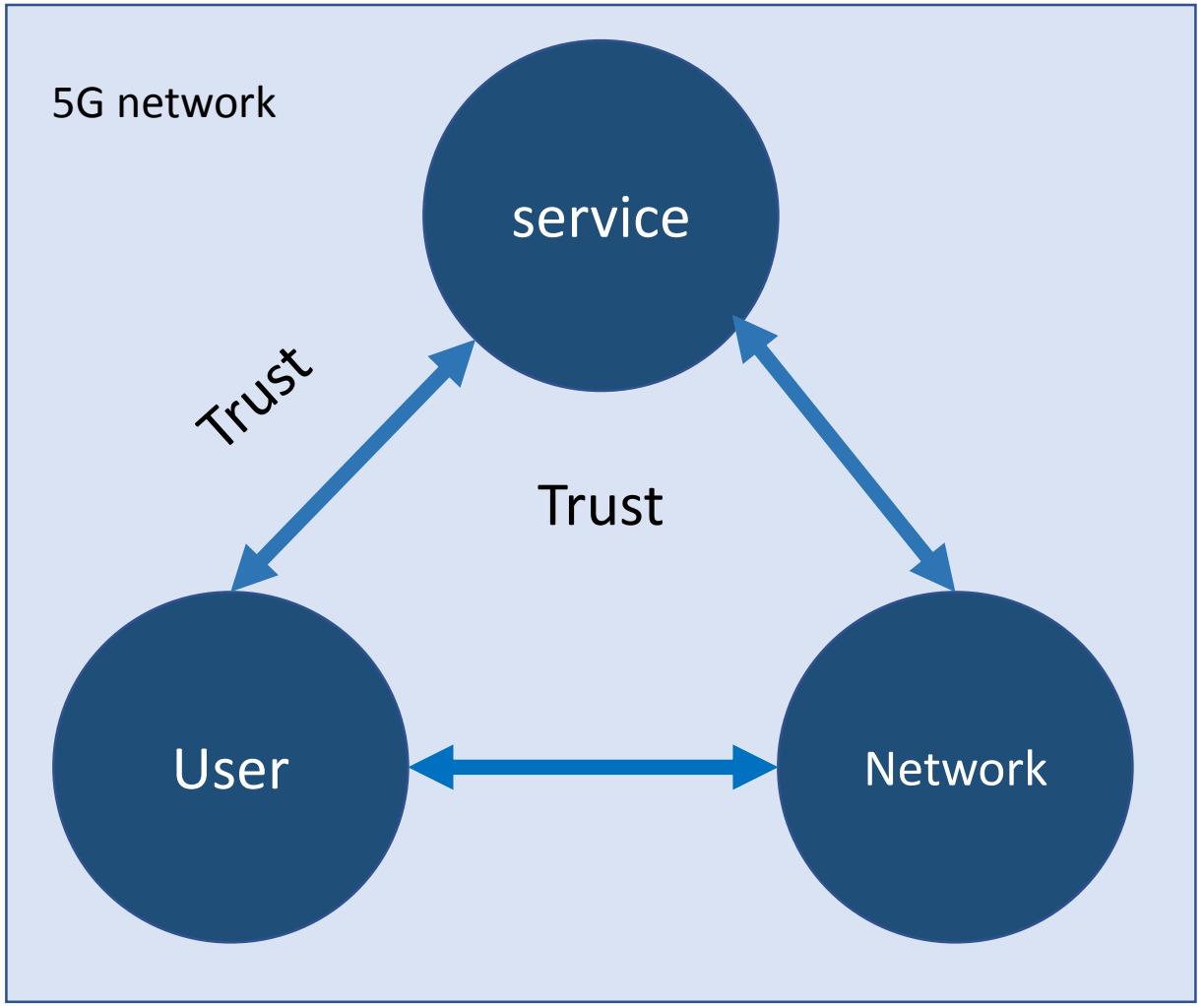
- *Endpoint protection* implements defensive capabilities on devices at the edge and in the cloud.
- Primary concerns include physical security functions, cyber security techniques and an **authoritative identity.**
- Endpoint protection alone is insufficient, as the endpoints must communicate with each other, and communications may be a source of vulnerability.

Endpoint protection

- ***Endpoint Physical Security*** provides physical protection of the endpoint with anti-tampering and theft prevention mechanisms to prevent uncontrolled changes or removal of the endpoint.
- ***Endpoint Identity*** is based on the inherent properties of an endpoint that distinguishes it from other endpoints.
- ***Endpoint Integrity Protection*** ensures the endpoint is in the configuration required to perform its functions predictably.
- ***Endpoint Access Control*** ensures that proper identification, authentication and authorization is performed prior to granting any resources or services.
- *Endpoint Secure Configuration and management* controls updates of security policy and configuration at the endpoint, including upgrades and patches of known vulnerabilities.
- *Endpoint Data Protection* provides controls to preserve the integrity, confidentiality and availability of its data.

New trust model and identity management





Communication and connectivity protection

- **Cryptographic Protection** uses cryptographic technologies to protect authenticity of communicating parties and integrity and confidentiality of exchanged data and metadata
- **Information Flow Protection** ensures that only permitted kinds of messages and content reach sensitive systems and networks by isolating network flows using network segmentation and perimeter protection technologies.

Security monitoring and analysis

- Monitoring
  - *Secure Remote Logging*:
  - Monitoring data is gathered by a local agent running on each of the endpoints and communications
- Analysis
  - *Rule-Based Analysis* monitors for violations of predefined policy rules that define events that should never occur in the system.
  - *Behavioral Analysis* observes the usage patterns in the system and learns what is appropriate behavior for the system.
- Act
  - Proactive / reactive responses
  - *Root Cause/Forensics* analysis and forensics

Security configuration and management

- Security Management is responsible for ensuring and executing the secure and controlled changes to the security policy and functions throughout the system. It should remain separate from Secure Operational Management.
- Endpoint Identity Management generates, updates and revokes machine (and user) principals and cryptographic materials (keys, certificates, etc.) used in the identification of the endpoint.
- Endpoint Configuration & Management is responsible for configuring and managing secure and controlled changes to the endpoint including both endpoint operational and security function.

Data protection

- Generally speaking data can be
  - Data at rest (DB, file systems, …)
  - Data in use (RAM, cache…)
  - Data in motion (network)
- Data must be protected against
  - unauthorized access and
  - uncontrolled changes
  - By applying functions such as confidentiality controls, integrity controls, access control, isolation and replication.

Security policy and regulation model

- The *Security Policy and regulation model* describes security objectives implied by regulatory, organizational, technical and other aspects
- For each of the currently mentioned building block there must be some kind of security policy
  - Standardization like ETSI, ISO, NIST…
  - Good practice and technical guidelines
  - Regulations like eIDAS, GDPR, ZInfV, ZKI…

Questions