Liability in 5G and Beyond: Concepts and challenges

Chrystel Gaber
Orange
WAL5Gplus 16/06/2021
Liability & 5G

- Service delivery in 5G:
  - Multi-party
  - Multi-domain
  - Multi-layer

- Dedicated services for critical & sensitive use cases ➔ verticals

Intelligent & automated support for liability management is needed

Source: Liability & computer security: nine principles, R.J. Anderson
Liability management - concepts

Liability

Accountability towards the law and stakeholders. For example contract law defines the accountability between the provider and the customer of a service.

Accountability

Set up of a governance to comply with responsibilities.

Responsibility

Task which needs to be performed while complying with a set of objectives. Incentives or penalties apply upon succeeding or failing to comply with objectives.

Governance

Definition of roles which have the right to perform specific actions (rights) with specific means (capabilities) as well as the evidences required to control actions.

Task

Objectives

Rights

Capability

Evidence / Transparency

Penalty

Incentive

For example contract law defines the accountability between the provider and the customer of a service.
Liability management challenges - 5G & verticals -

- Critical Verticals
  - are subject to NIS Directive & others specialized directives per segment (SEVESO, Transport, NIS2...)
  - have to manage / comply to safety and availability constraints

- Challenges & questions
  - How will infrastructure impact the commitments of critical verticals & how will vertical constraints be translated into agreements & contracts?
  - How liability will be transferred from critical verticals to network infrastructure operators and subcontractors?
  - How can a 5G slice management tool assist operationals & jurists?
  - How can we certify & insure 5G components & management systems?

We acknowledge that delivering on-demand or security contextualization of services is a key driver for 5G slicing adoption by critical verticals. Offers will have to embed liability (on-demand) between parties.
Thank you for your attention!

Find us at www.inspire-5gplus.eu

Twitter: @

Acknowledgment:
The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement № 871808. The European Commission has no responsibility for the content of this presentation.
Liability management & 5G Principles & Challenges

How will infrastructure impact the security commitments of critical verticals?

P2 - **Use the right threat model** - expect the real problems to come from blunders in the application design and in the way the system is operated

- Critical verticals are subject to **NIS directive** & others **specialized Directives per segment** (e.g. SEVESO, Transport, NIS2...)

P8 - **Security goals & assumptions** should be based on **industry practice** in the **application area**, not on general computer concepts

- Slice offers (on demand network capacities) need to address the different security requirements of verticals

Source: Liability & computer security: nine principles, R.J. Anderson
Liability management & 5G Principles & Challenges

How & what liability will be transferred from critical verticals to infrastructure operators and subcontractors?

- **P1** - Security systems (...) must be designed & certified on the assumption that they will be examined in detail by a hostile expert.

- **P3** - Security goals - Before setting out to build a computer security system, make sure you understand what its real purpose is.

- **P4** - Shifting the blame - Understand how liability is transferred by any system you build or rely on.

  - How can we avoid conflicting commitments & terms of use for service delivered to verticals?

  - How can we visualize the state of liability & responsibilities for each stakeholder of the system?
Liability management & 5G Principles & Challenges

How can a 5G slice management tool assist operationals & jurists?

P5- The limitations of the legal process & new kinds of technical evidences

P6- Computer security legislation is highly likely to suffer from the law of unexpected consequences

P7- Don’t rely on existing standards to solve legal problems

- Legal issues will not be solved only by a tool or standards. Is it possible to anticipate potential issues?

- What are the needs of auditors, experts, jurists to check evidences collected by a security, trust, liability system?

- What are the evidences related to autonomous & complex systems and how do their specificities impact the work of law makers & jurists?
How can we certify & insure 5G components & management systems?

P9: A trusted component or system is one which you can insure

- How can 5G providers convince their customers that if a component or system breaks and/or comprises the 5G system function or security, Service Providers will not lose an unpredictable amount of money or expose itself to lawsuits?
- Can we compose several components which are certified and/or insured to build a trusted service? (& how)?
Inspire5G+ paves the way for a liability management system

- Identified functions & enablers for a liability-management system

**F1 - Define accountability & relationships**
- Manifest
- Liability-Aware Security Manager
- Liability graph
- Behavioral profiles

**F2 – Monitor & collect evidence events / incidents**
- Root Cause Analysis
- Path Proof Protocol

**F3 – Analyse, resolve & identify liabilities**
- Liability-Aware Security Manager
- Liability graph
- Root Cause Analysis
- Risk Analysis Graph