Liability-Aware Service Management for 5G*

Presenter: Chrystel Gaber, Orange

Presentation at WAL5Gplus Workshop [Link]

Authors: Chrystel Gaber*, Jose Sanchez Vilchez*, Gürkan Gür†, Morgan Chopin*, Nancy Perrot*, Jean-Luc Grimault*, Jean-Philippe Wary*

*Orange Labs, Châtillon, France
†Zurich University of Applied Sciences, Wintertur, Switzerland

Introduction

- 5G is a technological revolution
  - flexible & dynamic network
  - enriched business cases with multiple layers & multiple parties
  - opening 5G infrastructure to third parties (e.g. IoT devices, VNF providers)
  - Slicing is an important technology enabler for 5G provided services

- Slice Provider is legally bound by contract to provide a QoS
  - financial & legal impact in case of fraud or mischief
  - security issues can have impacts on safety issues

- Managing liabilities and responsibilities in autonomous 5G infrastructure is key for its development and practical use
Introduction

- Example: operator offer enriched by partner

Fig. 1. Multi-party & multi-layer 5G infrastructure for service delivery

Introduction

- **Challenges**
  - worldwide deployment
  - multiple stakeholders
  - complex interconnections of hardware and software at different levels
  - orchestration across layers

- **Our proposal**:
  integration of liability as foundational element into the security management framework of 5G networks
  - Liability-Aware Security Manager
Related works

Responsibility-based Risk Management meta-model\(^1, \, 2\)

Security-by-Contract for Fog-based IoT\(^3\)

Security Panel\(^4\)

VNFD & NSD\(^5\), Security Manager \(^6\)

1- G. Guemkam, C. Feltus, C. Bonhomme, D. Kahdraoui and Z. Guessoum, “Reputation Based Dynamic Responsibility to Agent Assignment for Critical Infrastructure”, in 2011 IEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology
2- C. Bonhomme, C. Feltus and D. Khadraoui, “A multi-agent based decision mechanism for incident reaction in telecommunication network”, in ACS/IEEE International Conference on Computer Systems and Applications – AICCSA 2010
5- ETSI GS NFV-IFA 011 & 14
6- ETSI NFV SEC 024
Liability-Aware Security Management

Requirements for a LASM Infrastructure Manager

- Component Provider
- Service
- Service Manager
- User
- Service Administrator
- Slice Owner
- Contract
- Slice Provider
- Component Provider

Physical Device
VNF
Sub-Infrastructure
Validator

Component
Infra-structure
Component or Fleet
Component Manager

Supervises, acts on
Manages
Manages trust & liability policy
Provides KPI, Evidence
Provides SLA, SSLA
Manages updates & manifests

Validates
Once deployed, is part of
Listed in catalog or deployed as part of
Once deployed, may be part of

Uses

<5GWF-WS1, Bangalore, 10-12 Sept 2020>
Liability-Aware Security Management

- Strategic alliance between independent partners\(^1\)
  - each entity is independent
  - interaction of heterogeneous orchestration of each domain
  - unpredictable & uncertain impact on end-to-end service quality level

- Liability perspective
  - Identify domains or partners responsible for fault or outage
  - Encourage cooperation with penalties or incentives

---

Liability-Aware Security Management

User Plane
- LASM Visualisation Service

Monitoring & Reaction Plane
- LASM Analysis Service
- INSPIRE-5GPlus monitoring system

Security Orchestration Plane
- Manifest Class & Instance Descriptors
- INSPIRE-5GPlus Security Orchestrator
- LASM Referencing Service

Security Enforcement Plane
- INSPIRE-5GPlus Security Agents
Liability-Aware Security Management
Quelques captures d’écran de la démo
Challenges to achieve vision

- Accountability-related metrics

- Manifests
  - Distinguish levels of responsibilities: properties vs recommendations
  - Modular structure endorsed by multiple authors (Component Provider, Validators, Slice Provider)
  - *Manifest.Class* vs *Manifest.Instance*

- SLAs
  - Security SLAs for Slicing
  - Publicly-verifiable proofs of compliance
  - Automated incentives and penalties
Conclusion & future works

- Current work
  - Concept of Liability-Aware Security Management
  - Proposal Architecture for 5G slicing context

- Next steps:
  - Investigate identified challenges for each module
  - LASM Proof of Concept
  - Proposals related to manifests & security manager functional blocks to relevant IETF specification (IETF NFV-SEC 024, ETSI GS NFV-IFA 011 & 14)
Thank you for your attention!

Find us at www.inspire-5gplus.eu

Twitter: @inspire_5gplus

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.