Security Aspects in 5G framework – The SESAME Conceptual Framework

Evangelos Sfakianakis & Philippos Georgantas
(OTE - Research Programs Section, Fixed)

Infocom World 2016, Athens, Greece
November 02, 2016

Structure

- *Overview*
  - *SDN & NFV*
  - *Mobile Edge Computing (MEC)*
- *Existing Work on security and privacy for Cloud & MEC*
- *5G Concept*
- *SESAME- Actors*
- *SESAME functional architecture*
- *Security and Privacy Considerations*
- *Security and Privacy Considerations in SESAME concept*
- *UC - Enabling Large Multi-tenant Enterprise Services by Using MEC*
- *Security analysis of UC: View of CESC provider*
- *Security analysis of UC:* View of VSCNO

Overview

- A **novel architecture**, proposed for next-generation cellular networks will be presented. This architecture benefits from the recent advances in Software Defined Networking (SDN), Network Function Virtualization (NFV) and Mobile Edge Computing (MEC) which are natively integrated into the new and novel architecture.

- Approach based on EU-funded 5G SESAME project.

- SESAME aims at providing a fresh 5G mobile network architecture so as to support the ambitious goal of small cell virtualization, multitenancy and edge cloud services.
  The present work proposes a framework for security analysis applied in virtualised Small Cell (SC) Networks, with the aim of further extending MEC in the broader 5G environment.

SDN & NFV

- **SDN controllers** evolved operation and management of the network infrastructure
- **SDN helps virtualization** of the network infrastructure by facilitating isolation, abstraction and sharing of network resources

NFV provides several benefits such as:

- efficient management of hardware resources
- rapid introduction of new functions and services to the market
- ease to upgrade and maintenance
- exploitation of existing virtualization and cloud management technologies for VNF deployment
- reduction of CAPEX and OPEX
- enables a more diverse ecosystem
- encourages openness

Mobile Edge Computing (MEC)

- Decoupling control and data planes and abstracting network functions from physical infrastructure, brings greater flexibility to efficiently utilize radio and computing resources both in the Radio Access Network (RAN) as well as in the Mobile Core Network (MCN).

- ***MEC or "Fog computing", is a novel concept that extends the services, provided by the Cloud, to the network edge.***

- The available MEC infrastructure allows applications to run closer to the end user.
  This is expected to reduce the E2E network latency and to reduce the backhaul capacity requirements. Moreover, it enables better QoE of fast moving EUs, facilitates highly-interactive real-time applications, and even the emergence of novel applications, such as the Tactile Internet.

Initial Problem Definition for cloud – High Level

- **Everything goes cloud**
  - Consumer data like our emails or photos (google mail and other google services)
  - Public administration IT services
  - Soon all kinds of applications (incl. Critical Infrastructure - CI)
- Requirements for cloud applications vary
  - Commercial applications mainly focus on scalability & elasticity
  - Other Requirements regarding: overall redundancy, data availability, authenticity, secure access, trust and protection of the citizens are typically higher than in commercial applications.
- What is the problem?
  - Cloud services abstract over used resources, are opaque and make it hard to
    - *determine **technical** reasons for (security) failure and hence make the*
    - *development of countermeasures*
  - This also implies, from a **legal** perspective, that it is hard to
    - *determine who's fault it is and*
    - *to show one hasn't acted negligent*

Existing Work on security and privacy for MEC (1/2)

- **A number of security and privacy challenges of MEC have already been identified.**
- The considered **security threats** are mainly in the context of a cloud-*enabled* IoT (Internet of Things) environment. The study makes a classification of the available security technologies according to the involved network elements, such as technologies to secure a fog node (*i.e., the MEC server*) and an IoT node, as well as techniques to protect the communication.

- Other threats on the existing security mechanisms:
  - ***man-in-the-middle (MitM) attack and***
  - ***malicious fog node problem***.

- Assessment of authentication and authorization techniques **for connecting the fog with the cloud.**
- The applicability of existing techniques, such as **signature- and anomaly-*based* intrusion detection**

Existing Work on security and privacy for MEC (2/2)

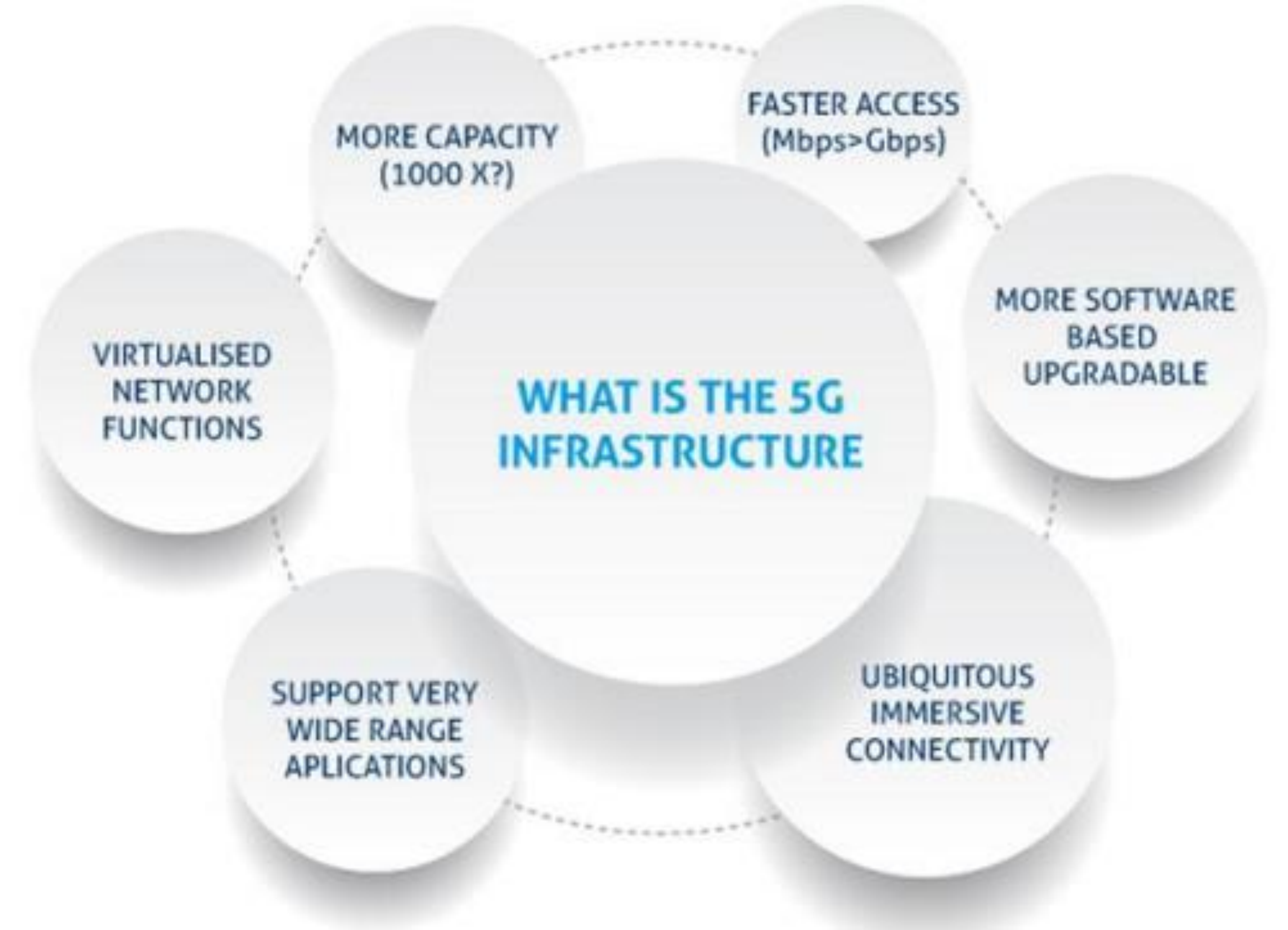
- **Challenges of MEC with respect to digital forensics** (sensors and various types of smart objects that require connectivity to the cloud and to each other)
- Processes and events that would allow reconstructing past activity for providing digital evidence.
- **Distinction between the techniques** that can be applied in both fog and cloud, and between those that are only applicable in one of them.
- Existing data protection techniques and their suitability in MEC.
- The conferred data theft attacks include both external intrusion as well as insider attacks.

5G Concept

5G is expected to assist an entirely mobile and fully connected and converged society

New capabilities of 5G dimensions

- *flexibility, lower energy requirements*
- *improved energy efficiency,*
- *greater capacity, bandwidth, security, reliability and data rates,*
- *enhanced indoor coverage*
- *lower latency and device costs*


WHAT IS THE 5G INFRASTRUCTURE
MORE CAPACITY (1000 X?)
FASTER ACCESS (Mbps>Gbps)
MORE SOFTWARE BASED UPGRADABLE
UBIQUITOUS IMMERSIVE CONNECTIVITY
SUPPORT VERY WIDE RANGE APLICATIONS
VIRTUALISED NETWORK FUNCTIONS

Source: http://5g-ppp.eu/about-us

SESAME- Actors (1/2)

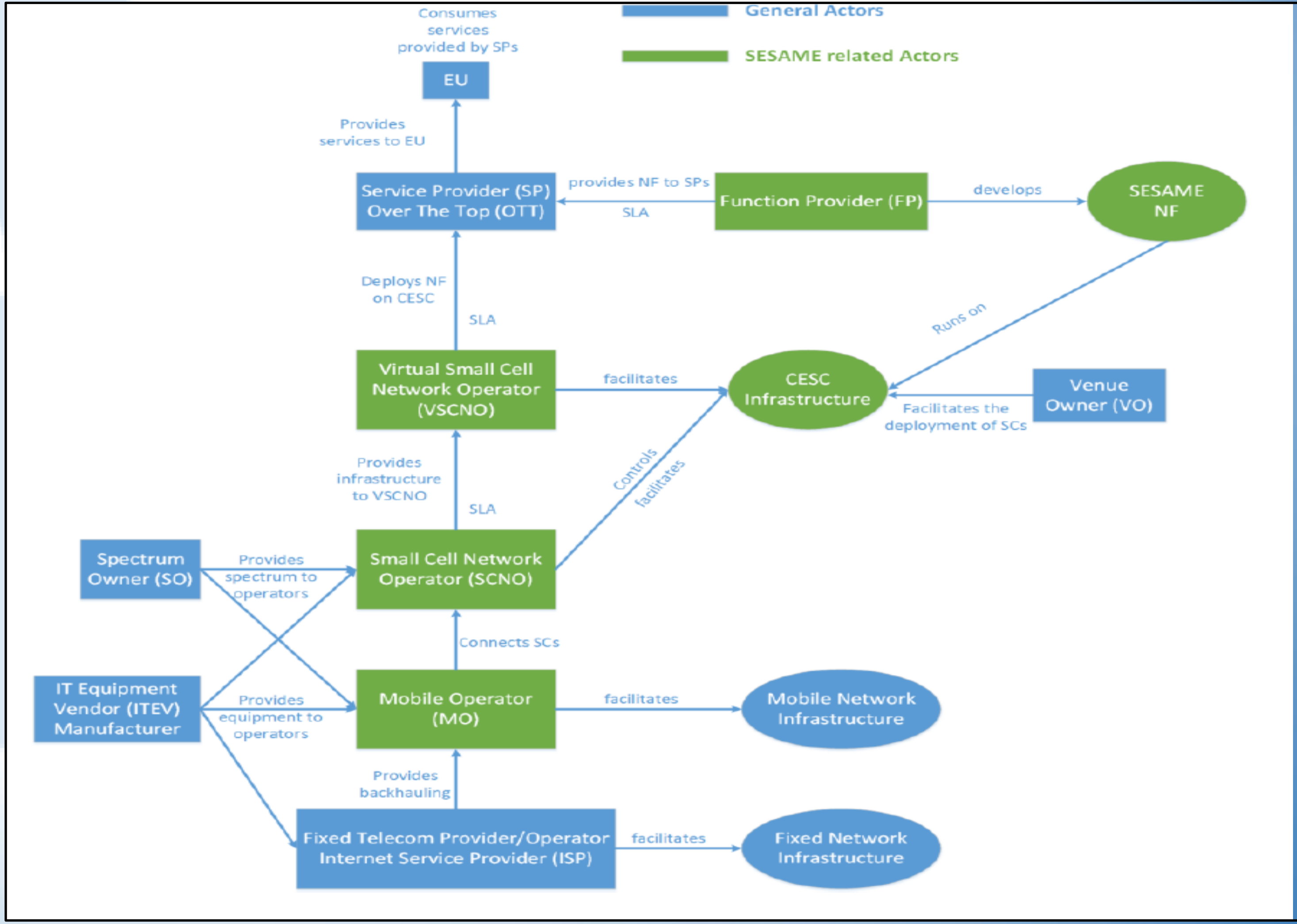
End User (EU): Mobile device.

Infrastructure Owner (IO): Owner of cellular infrastructure, (SCs, macro BS).

IT Equipment Vendor (ITEV): Entity who develops, manufactures or sells IT equipment(e.g.: BSs).

Small Cell Network Operator (SCNO): An entity that possesses equipment so as to provide radio communications services and that provides radio access to end-users locally, by using SCs.

Virtual Small Cell Network Operator (VSCNO): This entity does not possess the equipment but leases it from another one, so as to provide radio communications services and to deliver services to EUs.



General Actors
SESAME related Actors
Consumes services provided by SPs
EU
Provides services to EU
Service Provider (SP) Over The Top (OTT)
provides NF to SPs
SLA
Function Provider (FP)
develops
SESAME NF
Deploys NF on CESC
SLA
Runs on
Virtual Small Cell Network Operator (VSCNO)
facilitates
CESC Infrastructure
Facilitates the deployment of SCs
Venue Owner (VO)
Provides infrastructure to VSCNO
SLA
Controls facilitates
Spectrum Owner (SO)
Provides spectrum to operators
Small Cell Network Operator (SCNO)
Connects SCs
IT Equipment Vendor (ITEV) Manufacturer
Provides equipment to operators
Mobile Operator (MO)
facilitates
Mobile Network Infrastructure
Provides backhauling
Fixed Telecom Provider/Operator Internet Service Provider (ISP)
facilitates
Fixed Network Infrastructure

SESAME- Actors (2/2)

Macro- Cell Network Operator (MCNO): This possesses the equipment so as to provide radio communications services and provides radio access to EUs in wide areas at the macro cell level.

Backhaul Provider (BP): An entity that provides backhauling of the Small Cells and Macro Cells (e.g. ISP, MNO).

Service Provider (SP): An entity that produces, controls and distributes services over the MNO/VMNO.

Virtual Function Provider (VFP): This supplies virtual network functions (gateways, proxies, and transcoders). In this way, the need for the customer to acquire, install and maintain specialized hardware is essentially eliminated.

Spectrum Owner (SO): This entity owns a particular piece of spectrum in a given geographical area.

SESAME functional architecture (1/2)

MEC server: It is specialized hardware placed inside SC, that provides processing power, memory and storage capabilities and networking resources.

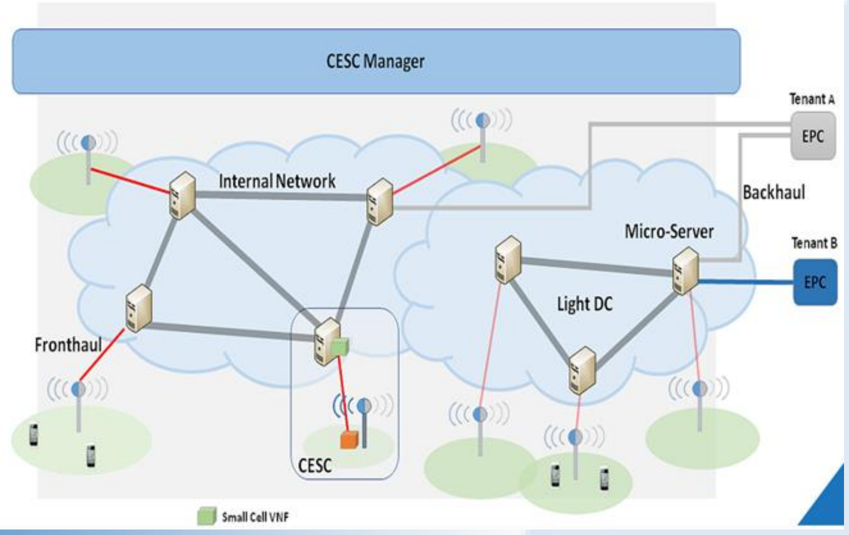
Cloud Enabled Small Cell (CESC): It is a SC device which has been enriched with a MEC server;
CESC cluster: A group of CESCs able to exchange Information.

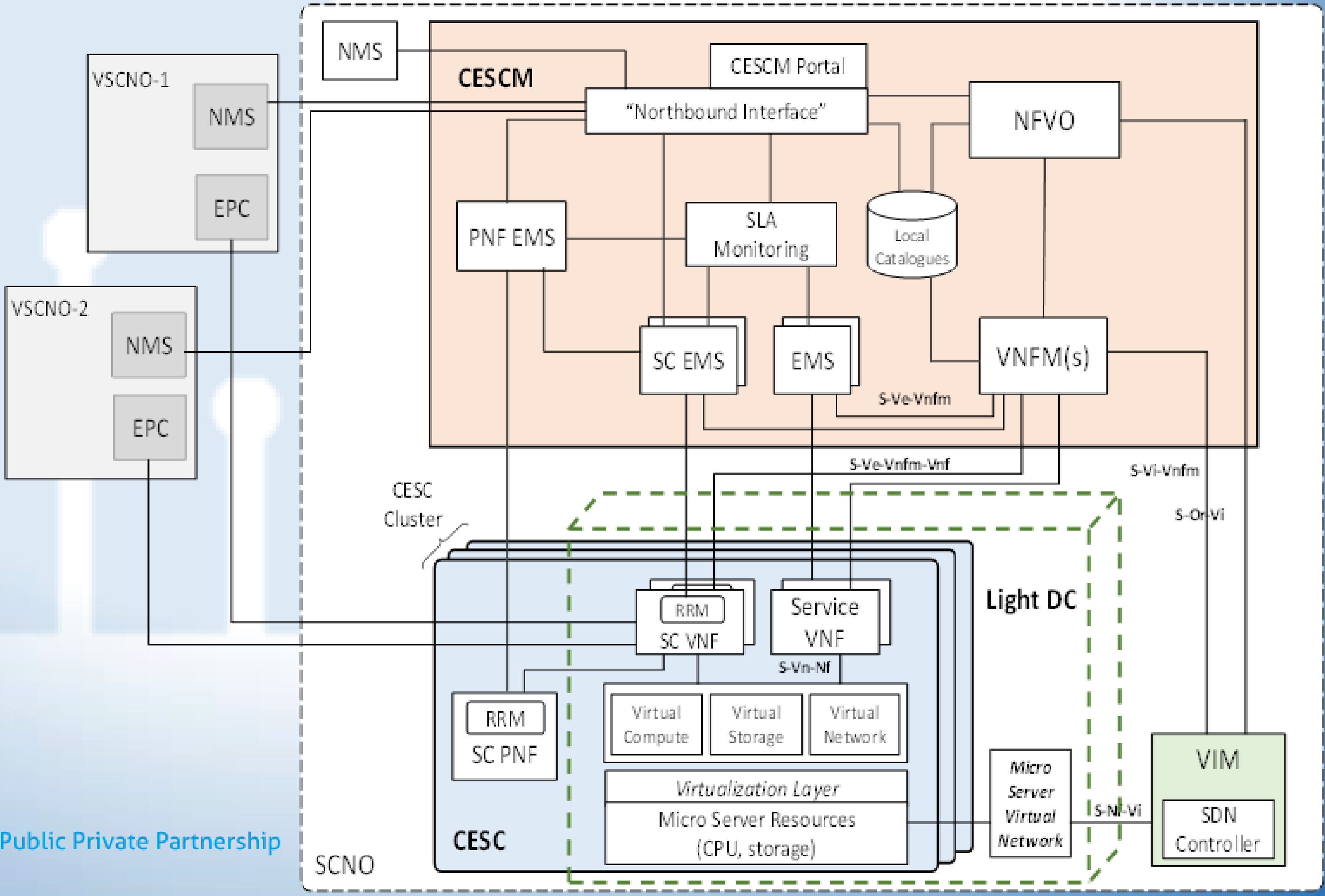
Light Data Center (Light DC): It is a cluster of MEC servers. This is a logical entity consisting of a set of distributed MEC servers of the same CESC cluster.

Virtual Infrastructure Manager (VIM): This manages virtual hardware (i.e., VMs) and networking resources of a single Light DC. The VIM is also responsible for the allocation of Virtual Network Functions (VNFs) over the hardware.

CESC Manager (CESCM): This is the architectural component in charge of managing and orchestrating the cloud environment of the Light DC; it can simultaneously manage multiple clusters, a cluster or a single CESC.
The CESC Manager also manages the radio access and "Self-x" functionalities.

SESAME functional architecture (2/2)





Security and Privacy Considerations

Security will be a fundamental enabling factor of future 5G networks.

Secure Tropos (SecTro): A methodology used to identify, model and analyse security issues from the early stages of system design and software development as well as to model and analyse threats and vulnerabilities in existing software

A cloud provider must ensure the physical security and integrity of the cloud infrastructure and of the data centres.

Cryptographic and privacy protection techniques need to ensure confidentiality and integrity of User Equipment (UE) data.

Security and Privacy Considerations in SESAME concept (1/2)

SESAME concepts can provide invaluable opportunities of developing solutions for attack prevention, management & recovery.

- ***Physical security of CESC has to be ensured***
- ***Attacks initiated from the cloud side*** (especially when multiple enterprises using private clouds are hosted
- ***Emerging Bring Your Own Device (BYOD) trend*** constitutes another threat
- ***Recommendations from the Cloud Security Alliance*** should be followed
- ***Adopted Public-Key scheme*** that enables the encryption of the communications among CESC, UE and the cloud, must be sufficiently secure.
- ***Cryptographic and privacy protection techniques*** are particularly important in cases where an EU receives service from multiple service or network providers, due to mobility or QoE considerations.

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION HORIZON 2020

The 5G Infrastructure Public Private Partnership

Security and Privacy Considerations in SESAME concept (2/2)

SESAME concepts can provide invaluable opportunities of developing solutions for attack prevention, management & recovery.

- **NFV Orchestrator is an attractive attack target** due to being in the “middle” of the system model architecture;
- So is VNF Manager.

- Considering virtualised environment, **both host and guest Operating Systems (OSs) may be targeted and to alleviate the impact of such attack**, adequate isolation must be enforced between guest VMs, as well as between the host and guest VMs.

- **Identifying and mitigating security threats and vulnerabilities at the intersection of MEC with “Small Cells-as a-Service” (SCaaS), SDN, and NFV is crucial.**

Enabling Large Multi-tenant Enterprise Services by Using MEC (1/2)

SCNO provides radio interface to mobile operators, virtual mobile network operators (VMNOs) and VSCNOs.
SCNO may transmit by using licensed or unlicensed spectrum
SCNO offers a platform for MEC for low latency and compute intensive applications.
MOs, VMNOs and VSCNOs provide both in-house and third party services from OTT players or the SPs.

CESC is comprised of:

Hardware resources:
Virtualization layer: abstracts the hardware resources and decouples the VNF software from hardware
VNFs: virtualization of a network function in a legacy non-virtualised network
Element Management System (EMS): performs management of one or more VNFs.

A cluster of CESCs is managed by the CESCM that constitutes of:

VIM: manages the interaction of a VNF with the compute, storage and network resources under its specific authority.
VNF manager: is responsible for VNF management.
Network functions virtualisation orchestrator (NFVO): is in charge of orchestration, of management NFV infrastructure and software resources and of realizing network services.

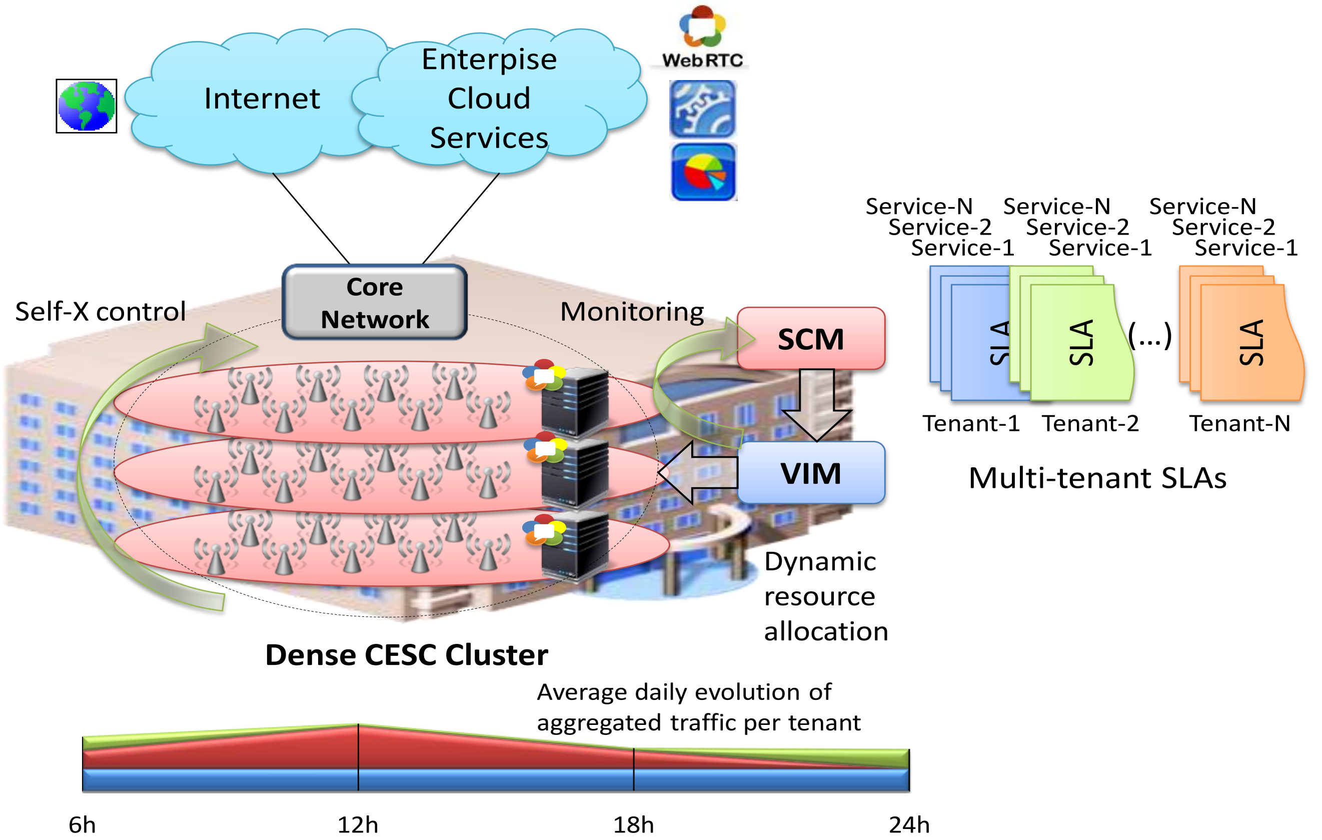
Enabling Large Multi-tenant Enterprise Services by Using MEC (2/2)

A CESC provider has Service Level Agreement (SLA)

The deployment of MEC servers with high processing capabilities can enable close-to-zero latency and enhanced QoE of the enterprise users. MEC servers can provide storage resources and support content caching at the network edge.

This scenario will leverage on SESAME features *-such as multi-tenancy-* by enabling multiple Small Cells operators to provide network services and connectivity over the network owned by a single CESC infrastructure provider.

Backhauling is required.

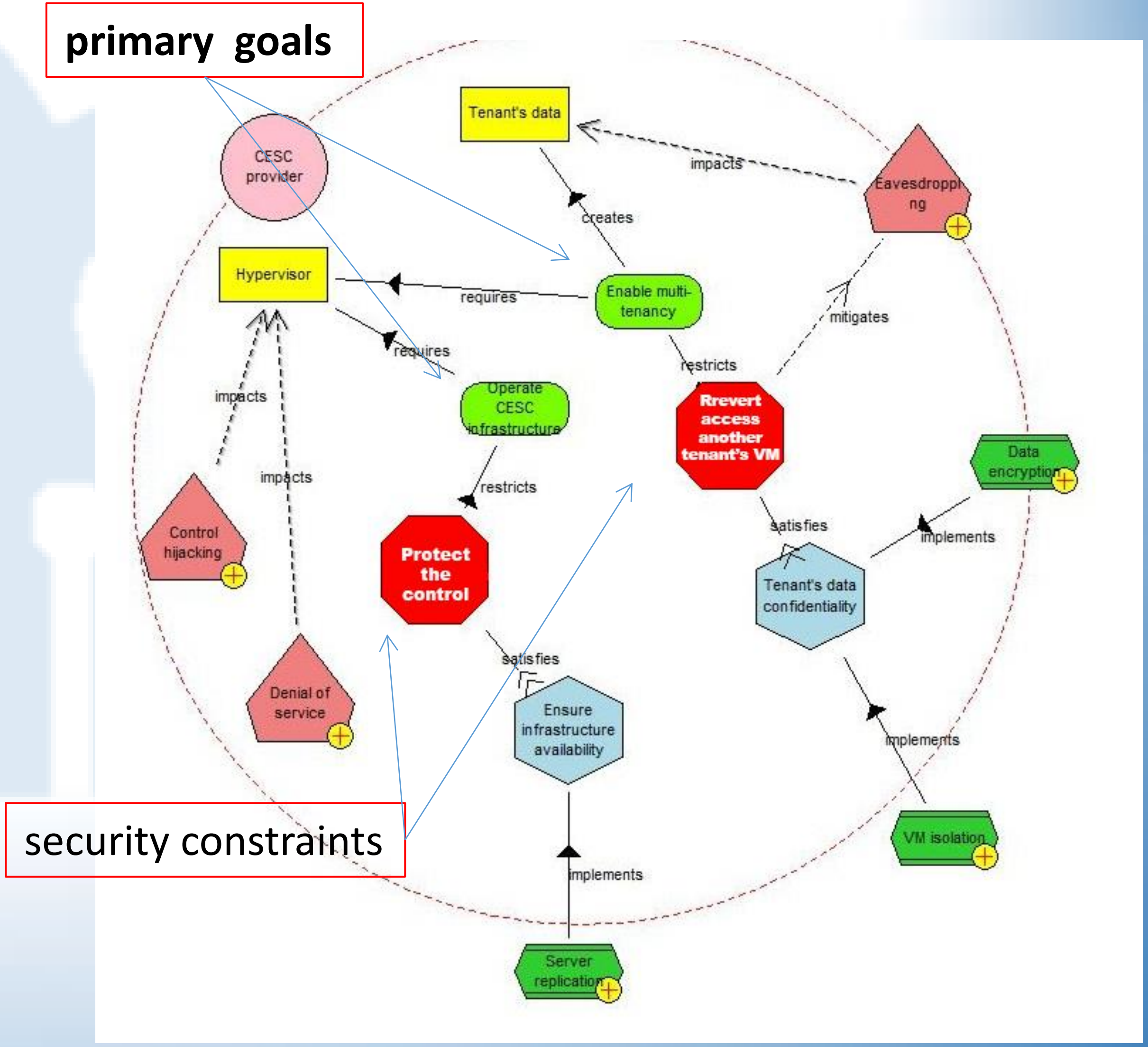


Security analysis of UC: View of CESC provider

Hypervisor and Tenant's Data need to be protected
A resource must achieve a specific "goal" of an actor (CESC provider). **These goals (green)** require the Hypervisor as a primary resource. To enable multi-tenancy, the Tenant's Data resource has to be created. A goal could be restricted by a "**security constraint**" (**red octagon**).
Various security constraints must satisfy a number of "security objectives" (**blue hexagons**).

Security constraints are satisfied by the two objectives: **Protect the Control Plane** and **Prevent Access to another Tenant's VM.** These objectives are implemented by using a number of "**security mechanisms**" (**green hexagons**).

"**Threats**" (**pentagons**) impact resources.
Hypervisor has two threats: **Control Hijacking** and **Denial of Service.**
Tenant's Data resource can be impacted by the **Eavesdropping threat.**



primary goals

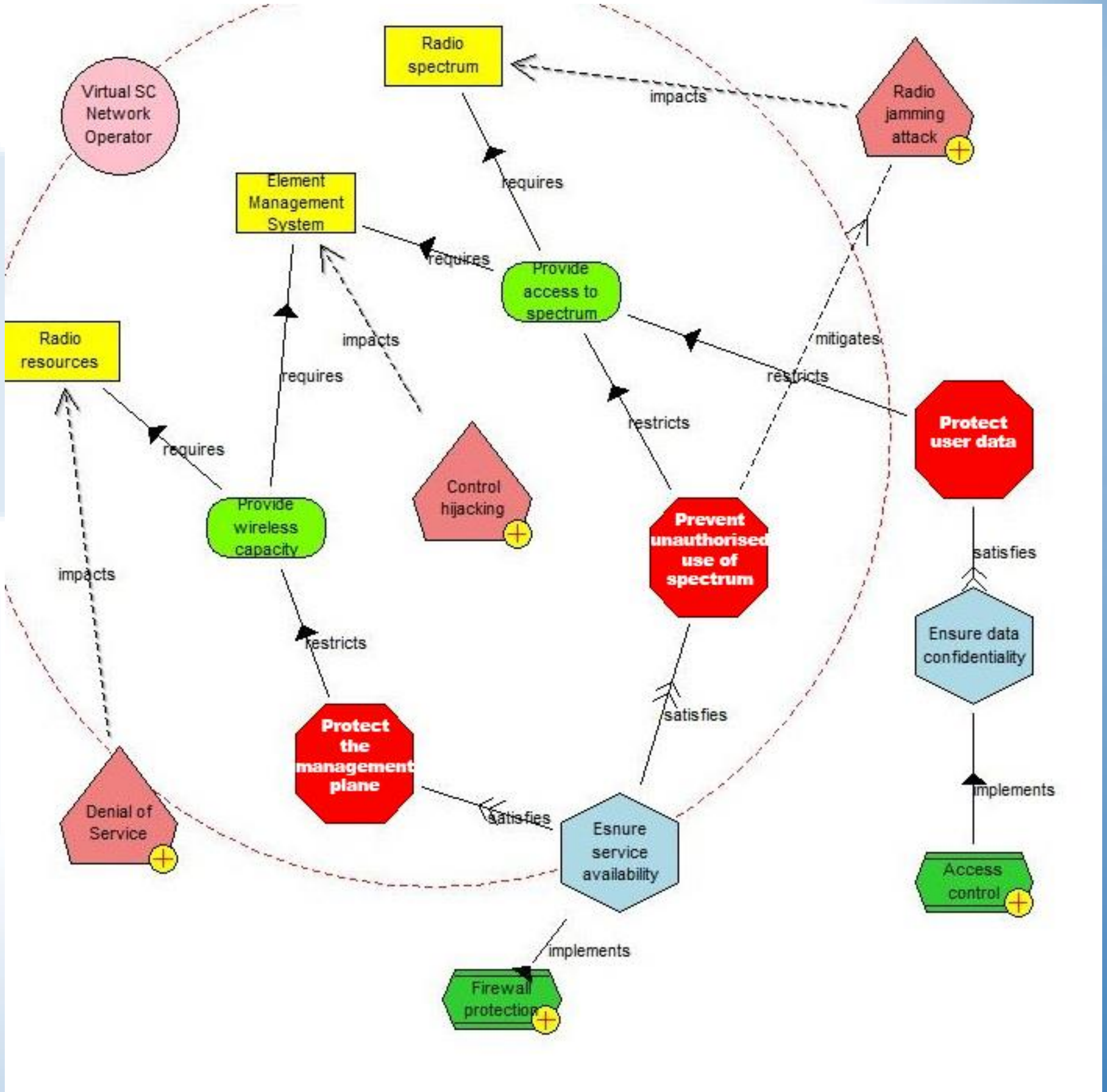
security constraints

Security analysis of UC: View of VSCNO

The security component view of the VSCNO, contains three resources that need to be protected: the **Radio Resources**, the **Radio Spectrum** and the **EMS**.

Actor's primary goals: **Provision of wireless capacity** and **spectrum to the tenants.**

Security constraints that restrict these goals are to **protect the management plane**, to **prevent unauthorized access to the wireless spectrum and to protect user data.** These constraints **must be satisfied** by two security objectives: **Ensure service availability and data confidentiality.**
Security mechanisms are using firewalls and access control mechanisms.
A number of threats could impact the considered resources, such as **DoS, control hijacking** and **radio jamming attacks**.



Q & A

For further information:

Ioannis Chochliouros, Ph.D., M.Sc., *ichochliouros@oteresearch.gr*

(Head of Research Programs Section, Fixed – Coordinator of the SESAME Project)

Evangelos Sfakianakis, M.Sc. *esfak@oteresearch.gr*

Research Programs Section, Fixed

Hellenic Telecommunications Organization S.A. - OTE

SESAME Project website:

http://www.sesame-h2020-5g-ppp.eu/