Tutorial Proposal

1. Email:

bmsousa@dei.uc.pt

2. Title:

Trusted Service Function Chaining for Mission Critical Services

3. Abstract:

Mission Critical Services (MCS) are characterized by stringent requirements due to the criticality of the mission being performed. MCS can rely on different types of services, which include voice communications, video, data flows from sensors, location devices, among others. Service Function Chaining (SFC) enables the delivery of end-to-end services with distinct functions that can have multiple dependencies and different security requirements. SFCs consider the order on which functions must be executed/traversed and the components on which such functions are deployed, for instance if deployed at edge or cloud nodes. SFCs are commonly deployed using approaches that explicit the composition, the order of functions, but do not provide mechanisms to dynamically adapt the composition of services (e.g. add new function to a deployed service). Mission Critical applications have heterogeneous requirements. For instance, services in vehicular networks to support autonomous driving, monitoring critical infrastructures like smart grids, require low latency, high levels of security. On a safety perspective, Mission Critical Push To Talk Services in Smart Cities also require fast/flexible setup of groups, while the data services, require aggregation points due to the high data volumes. Thus, diverse MCS services can share a set of service functions (e.g., security) but the specificities associate with each service function must be considered. In this regard, Service Function Chaining for MCS needs to support adaptive composition and migration of service functions due to aspects such as availability of nodes and location updates. Indeed, the placement and chaining of service functions must be performed in a way that maximizes resilience, minimizes end-to-end latency, while considering constraints related to resource availability and trust in nodes and service functions.

4. Objectives:

The objectives of the tutorial are:

- Provide insights regarding the composition of functions for Service Function Chaining in different platforms (OpenStack, Kubernetes) for Mission Critical Services.
- Present a comprehensive description of mechanisms to enable trust on service functions and nodes providing resources for Service Function Chaining.
- Hands-on on CloudSimSDN simulator (https://github.com/Cloudslab/cloudsimsdn) to simulate scenarios with SFC policies.

5. Topics covered:

The topics covered with the tutorial are the following:

- **Secure computing and secure architectures (as per the ISCC call for tutorials).** The motivation of the tutorial is aligned with the need for mechanisms that assess the reputation on nodes and service functions that compose SFCs. Services can be orchestrated using different paradigms, as Virtual Network Functions (VNFs), as Container Network Functions (CNFs), nonetheless their placement and distribution needs to consider trust information, so that sensitive functions (e.g. login) are not placed on nodes with questionable reputation.

- **6G and wireless Communication technologies (as per the ISCC call for tutorials).** The motivation in this topic is aligned with the current evolution of 5G, for URLLC to enhance the deployment of services with stringent latency requirements and high reliability. In addition, 5G is already promoting the virtualization of services, in the VNF paradigm, with a tendency to move to CNF deployment paradigm, several projects propose solutions for Open RAN based on container technologies, as the example of SD-RAN from ONF. This tutorial aims to consolidate the know-how on how to chain and place service functions for next generation communication technologies.
- **Smart cities (as per the ISCC call for tutorials).** The motivation in this topic in aligned with Mission Critical Services, that can leverage from information existing in devices that support smart cities, smart lamps that detect pedestrians crossing streets, vehicles that might have an accident and share their accurate location with rescue teams. In this regard, nodes, devices and service functions responsible to share data need to be trust full (topic 1) to avoid false emergency calls.
- **Software Defined Networks and Network Functions (NF).** The motivation in this topic is aligned on how policies for NF can be implemented with using Service-Mesh approaches in Kubernetes for functions in Containers – CNFs or employing the paradigm of functions deployed in Virtual Machines – VNFs managed by orchestration platforms like OpenStack, OSM, among others.

6. Projected Audience/Background:

Tutorial attendees should have background knowledge on networking concepts such as routing and Internet applications and services. In addition, knowledge on simulation is also helpful.

7. Tutorial content:

1. Introduction
1.1. Objectives
1.2. Motivation for Service Function Chaining
2. Mission Critical Services
2.1. Modelling services
2.2. Advances in communication technologies (5G)
3. Service Function Chaining
3.1. Standardization in SFC
3.2. Virtualization paradigms (CNF, VNF) and issues
3.3. Edge and cloud continuum aspects
4. Trust in Service Function Chaining
4.1. Modelling trust
4.2. Attesting the functionality of an entity
4.3. Building reputation
5. Case Studies
5.1. Smart Cities use cases (OREOS and SNOB5G)
5.2. Smart Grids use cases (Smart5Grid and ELEGANT
5.3. Attestation and Reputation Systems (ARCADIAN-IoT and AIDA)
5.4. Hands on simulation
6. Discussion

The description of the planned program is as follows:

1. Introduction (15 minutes)

This topic aims at motivating the attendees to the topics addressed in the tutorial.

1.1. Objectives

This module provides information regarding the goals of the tutorial

1.2. Motivation for Service Function Chaining

This module provides information regarding the motivation for Service Function Chaining in 3 main scenarios, with demanding requirements. This module also presents examples on how Service Function Chaining can enhance the deployment of services in Smart Cities and SmartGrids.

2. Mission Critical Services (30 minutes)

This topic aims to provide information regarding the complexity of critical services, in particular when they involve safety and the advances that have been made in communication technologies to support such services.

2.1. Modelling services

This module details aspects related with the requirements of critical services, and how reliability, availability, security aspects can be modelled. For instance, reliability is modelled in Service Level Agreement (SLA) perspective, such as 99.99% availability, also includes information regarding the protection model of Service Function (e.g. fully redundant, or in a primary-backup model). Aspects related with the modelling and architecting services and identifying critical functionalities are discussed in this sub-topic.

2.2. Advances in communication technologies (5G)

The advances in communication technologies like Ultra Reliable low latency communications (URLLC) in 5G, Direct Mode, Mission Critical Push to Talk (MCPTT) are discussed in this module. The information covered in this module focus mainly, safety services, with communications with high requirements of reliability and low latency.

3. Service Function Chaining (45 minutes)

This topic aims to introduce SFC, the current standardization efforts, the challenges in the diverse deployment paradigms, as well as how policies can be modelled to enable edge-cloud continuum.

3.1. Standardization in SFC

This module aims to present the current work on IETF SFC working group regarding the Service Function Chaining, the specification of ETSI regarding the forwarding graphs for Virtual Network Functions.

3.2. Virtualization paradigms (CNF, VNF) and issues

This module aims to introduce the challenges of SFC within the different virtualization approaches, in particular those relying on containers orchestrated by the Kubernetes platform - CNFs, as well as those related with Virtual Network Functions managed through platforms like OpenStack, OSM and others - VNFs. The composition of service function, the policies to enable SFCs are presented in this module considering the trends like service mesh concepts to enhance reliability of CNFs. The issues regarding hybrid deployments are also discussed, in terms of collecting data to properly orchestrate service function, and the enforcement of policies.

3.3. Edge and cloud continuum aspects

This module aims to present the solutions to enable edge deployment like KubeEdge, and its interconnection with the cloud. The aspects related with the placement of service functions to place functions close to the user, to reduce latency but considering security constraints are also presented here. The policy enforcement through software defined networks (SDN) is also considered here.

4. Trust in Service Function Chaining (30 minutes)

This topic aims to describe the approaches to enable trust in Service Function Chaining and related resources (nodes where service functions are placed). Thus, dealing with mechanisms that attest the functionalities of entities to build reputation.

4.1. Attesting the functionality of an entity (Service Function, nodes)

This module includes information regarding lightweight attestation approaches that ensure that Service Functions operating in distinct nodes can be verified, as well as the behaviour integrity of nodes hosting service functions. The attestation mechanisms can be based on diverse techniques like challenge-response approaches, that need to consider the nodes profiles (e.g computational capabilities), where functions are hosted. Along with the attestation mechanisms, robust and efficient identification mechanisms need to be devised/developed to establish reputation models that enable the verification of nodes requesting a specific service, but also allowing nodes hosting service functions to assess the trust of service requesters. This module details the approaches to distribute the information of reputation models in a decentralized fashion and considering the diverse entities that interact with Service Functions (users, nodes, etc).

4.2. Federated Authentication (OpenID Connect)

This module provides information on how authentication can be performed in service functions, using federated mechanisms enabled by OpenID Connect. The authentication aspects, supported by OAuth 2 are also considered here, and their interconnection with SFC and related technologies like Software Defined Networks (SDN).

5. Case Studies (45 minutes)

This topic describes case studies of projects where the author and presenter of this tutorial is leading research activities.

5.1. Smart Cities use cases (OREOS and SNOB5G)

These projects aim to enable an orchestration platform for services in smart cities using diverse technologies like 5G, mmWave. These projects aim to enable orchestration exploits multihoming aspects (multiple and heterogeneous connections to the core network), and considering the restrictions services involved with the safety of people (pedestrians crossing streets).

5.2. Smart Grids use cases (Smart5Grid and ELEGANT)

This project targets services in critical infrastructures, such as SmartGrids in 5G networks, that can be used in distinct models (in a public mode, non-public mode, standalone, etc). The use case in this project is relevant to illustrate the complexity of modelling critical services for demanding environments.

5.3. Attestation and Reputation Systems (ARCADIAN-IoT and AIDA)

These projects tackle authentication mechanisms, using different approaches, biometrics and OpenID connect, to security in communications. The project ARCADIAN-IoT, also considers the heterogeneity of devices and the need for attestation mechanisms to build trust and reputation of diverse entities (services, nodes, persons).

5.4. Hands on simulation

This module aims to introduce the attendees of the workshop in a simple scenario that is simulated in CloudSimSDN. Attendees have the option to follow the presenter in the simulation workflow. Instructions to perform simulation are shared with attendees for their own future experiments and to optimize the time management in the tutorial.

6. Discussion (15 minutes)

This topic briefly summarizes the topics previously discussed in the tutorial and provides guidelines for the next steps towards the implementation of SFC in the context of Mission Critical Services.

8. Presenter Experience:

This is the first tutorial attempt in a conference by the author. Nonetheless, the author has performed already other presentations with the same level of demanding as the tutorial in the PhD and master classes, as well as in the international research projects, such as SALUS, MobileCloud and more recently in SNOB5G.