CHARISMA

CHARISMA NEWS

#8 – November 2017

Editorial

Dear Reader,

This is the eight issue of CHARISMA News, the newsletter of the Horizon 2020 5G-PPP Project CHARISMA: **C**onverged **H**eterogeneous **A**dvanced 5G Cloud-**R**AN Architecture for **I**ntelligent and **S**ecure **M**edia **A**ccess.

This edition focuses on the latest CHARISMA results and the dissemination activities that have taken place in the past few months.

I hope you will find the contents of this newsletter interesting. Your comments and suggestions are, as always, appreciated.

Dr. Theodoros Rokkas (INCITES CONSULTING, trokkas at incites.eu), Editor

Project results & activities

CHARISMA 5G v-security prototype

The CHARISMA 5G v-security solution targets the demonstration of how a leased network slice in a 5G network could benefit from NFV-based virtual security functions along with automated security management features. The VSFs (vFW and vIDS), NFV Orchestrator, the Security Policy Manager (SPM), and Monitoring & Analytics, together form the CHARISMA v-security solution. These modules are developed and extended as components of the CHARISMA CMO.

The CHARISMA content caching and traffic handling solution is realized as an NFV-based network service provisioned through the NFV orchestrator over a particular slice. The network slicing feature in CHARISMA CMO is achieved through the Open Access Manager, which is tightly knitted with the rest of the components to enable isolated network slices for different VNOs for the provisioning of security or caching services.

The development of the CHARISMA CMO has been successfully completed and verified by deployment in the NCSRD testbed. The development was carried out in incremental phases with module dependencies in mind. During the development of the CMO modules functional tests were conducted per module to ensure the desired functionalities. In addition, module integration tests were designed and performed to ensure inter-module working. The caching (vCC and vCache) and security services (vFW, vIDS) were provisioned on the testbed via the CHARISMA GUI to validate the final prototype.

CHARISMA E2E V-security Architecture

Future 5th Generation (5G) technologies are anticipated to address next-generation communications networking challenges and

Project Coordinator: Dr. Eduard Escalona, i2CAT Fundació • eduard.escalona at i2cat.net
Technical Manager: Dr. Michael Parker, University of Essex • mcpark at essex.ac.uk
Dissemination Leader: Dr. Theodoros Rokkas, INCITES CONSULTING • trokkas at incites.eu

tackle the novel business requirements associated with different vertical sectors. It is anticipated that convergence, automation and flexibility are expected to be intrinsic traits of any 5G system. The introduction of this multitude of complex new requirements and novel technologies will immensely impact the security landscape of 5G, and therefore the need to revisit network security properties becomes essential. The security vision for 5G will, at the least, consist of the collection of security landscapes for all involved technologies (wired or wireless networks, virtualization, etc.) and the vertical sectors. However, analysing the complete security landscape for all involved technologies and vertical sectors in 5G is out of the scope of this newsletter. However, in this document we shall revisit the security aspect for CHARISMA architecture by focusing on the end-to-end virtualised security (v-security) architecture.

The CHARISMA architecture targets 5G access networking and enables an infrastructure owner to share their network with multiple virtual network operators (VNOs) through network slicing. Moreover, CHARISMA tightly knits the network slicing concept with the SDN/NFV environment in its infrastructure to facilitate a VNO's fast track provision of network services on their leased-out network slices. [Reminder: A network slice in the CHARISMA architecture consists of both compute and network resources. Furthermore, the CHARISMA architecture considers both virtualized as well as physical resources in its infrastructure given the SDN/NFV environment.] The intelligence driven v-security solution provides a virtualized security defence from a network services perspective, enabling virtual security functions, security policy management, and security monitoring on a per-service basis. However, for an end-to-end virtualized security blanket in an SDN/NFV-based multi-tenant environment, control-plane slicing and its security aspects also need to be considered in addition to the network service level v-security.

In deliverable D2.5 "CHARISMA e2e v-security architecture" we have provided the description of the CHARISMA security solution that has shaped our final 5G architecture design. In particular, we describe the available key distribution protocols, as well as the encryption and decryption functions available to us, while ensuring the low-latency operation of the network. In addition, the design and implementation of our virtualised-security approach, based upon CHARISMA's virtualised infrastructure and control, management and orchestration (CMO) architecture is described.

The D2.5 deliverable focuses on the security of SDN-enabled control-plane slicing which combines with the intelligence driven v-security solution, to constitute the end-to-end v-security architecture. D2.5 describes the concept and functional requirements of control-plane slicing, to perform a threat analysis that in turn enables the identification of security requirements. The document proposes a solution and discusses how it could be adapted to the CHARISMA control-plane architecture along with the description of the required key exchange mechanism.

Project Coordinator: Dr. Eduard Escalona, i2CAT Fundació • eduard.escalona at i2cat.net
Technical Manager: Dr. Michael Parker, University of Essex • mcpark at essex.ac.uk
Dissemination Leader: Dr. Theodoros Rokkas, INCITES CONSULTING • trokkas at incites.eu

Apart from the end-to-end virtualized security, the document also surveys the security aspects of the other layers of the stack in a 5G network, in general. This provides the reader with an overall view of an end-to-end security architecture suitable for 5G networking.

Dissemination Activities

Open Event

CHARISMA and Telecom Slovenije organized an Open Event on Wednesday 29/11/2017.

The event took place at the TS premises in Ljubljana and included short presentations along with a live demonstration highlighting the achievements that have been made in the CHARISMA project. The audience coming from the local telecommunications and hi-tech sectors had the opportunity to get informed about the various aspects of CHARISMA such as:

- SDN/NFV-based End-to-End Network Slicing for 5G Multi-Tenant Networking
- Techno-economic modelling of 5G networks
- Caching advantages and perspectives for 5G networking
- An introduction to OFDM-PON for 5G converged optical access
- TrustNode, a versatile research router platform for 5G networking and routing
- 5G CHARISMA architecture towards future connected and autonomous vehicles
- Connected Autonomous Vehicles (CAVs): Safety and Security

More info can be found at: CHARISMA open event

Summer School

CHARISMA and the Faculty of Electrical Engineering at University of Ljubljana also organized the 3rd CHARISMA Summer School: "Fixed-Mobile Convergence in 5G Networking" at Ljubljana on 30/11/2017. Participants had the opportunity to interact with researchers and academics from several European Universities, Research Institutes and Industry.

The lectures covered the following topics:

- TrustNode, a versatile research platform for 5G networks
- Introduction to Techno-economic modeling for 5G networks
- Caching advantages and perspectives for 5G
- 5G CHARISMA architecture towards future connected and autonomous vehicles
- An introduction to OFDM-PON for converged optical access
- Fixed-Mobile Convergence in 5G Networking

More info can be found at: CHARISMA 3rd Summer School

About CHARISMA

The CHARISMA project is funded by the European Commission (Horizon 2020 program) within the 5G Public-Private Partnership (5G-PPP) initiative under the grant agreement No: 671704.

Project Coordinator: Dr. Eduard Escalona, i2CAT Fundació • eduard.escalona at i2cat.net
Technical Manager: Dr. Michael Parker, University of Essex • mcpark at essex.ac.uk
Dissemination Leader: Dr. Theodoros Rokkas, INCITES CONSULTING • trokkas at incites.eu