Applying Security Service Level Agreements in V2X Network Slices

Ricard Vilalta*, Pol Alemany*, Roshan Sedar*, Charalampos Kalalas*, Ramon Casellas*, Ricardo Martínez*, Francisco Vázquez-Gallego*, Jordi Ortiz†, Antonio Skarmeta†, Jesús Alonso-Zarate* and Raul Muñoz*

*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels, Spain
†University of Murcia, Murcia, Spain

Abstract—This demo presents the instantiation of a high level architecture proposed by INSPIRE-5Gplus to manage secured End-to-End (E2E) Network Slices. Network Slices are associated with Security Service Level Agreement (SSLA) to enhance the security on the virtual deployed resources, thus securing the created E2E Secure Network Slices. The proposed secured network slicing architecture is validated against a vehicular scenario, based on Anticipated Cooperative Collision Avoidance use case. In this scenario, we propose to detect false vehicular messages through a novel SSLA based on an Intrusion Detection System. The demo provides measurement of significant metrics such as mean time to detect, mean time to contain, and transaction speed.

I. INTRODUCTION

A Security Service Level Agreement (SSLA) aims at the definition of a set of requirements to ensure the safeness of a service (e.g., information integrity or encryption) in front of a possible problem affecting the information and accessing the service. An SSLA machine readable format has been detailed on the SPECS SSLA model to support slicing [1].

An initial architecture to manage End-to-End (E2E) Network Slices which, once deployed, are associated with SSLA(s) to increase the security on the virtual deployed resources and create End-to-End Secure Network Slices was presented in [2]. The Security Manager (Mngr) takes care of the SSLA lifecycle in a Slice: a) it gathers the verticals/end-users security requirements; b) deploys the necessary security functions to enforce the agreed SSLA by enriching or configuring the SPs’ services; c) monitors in real-time the SSLAs fulfillment; d) detects violations in security provisioning level based on an analytic engine and notifies both end-users and SPs; and e) reacts in real-time to adapt the provided level of security or to apply proper countermeasures.

In order to find a suitable scenario to deploy the SSLA in a network slice, this demo proposes the introduction of an emerging vehicular scenario, with Cooperative-Intelligent Transport Systems (C-ITS) [3]. Two types of messages have become the basis for C-ITS services: a) Cooperative Awareness Message (CAM), a periodic message that provides status information to interested actors; and b) Decentralized Environmental Notification Message (DENM), which is triggered only to notify a safety-related event. A high-level description of the Anticipated Cooperative Collision Avoidance (ACCA) system architecture and functionalities that makes extensive use of CAM and DENM messages is provided in [4] and [5].

In this demo, we propose to show the clear benefits of continuously evaluating the proposed SSLA in the deployed vehicular network slice (V2X) in order to assess vehicle trustworthiness. This can trigger the decision of removing vehicular DENM messages. Finally, the demo provides measurement of important performance metrics such as mean time to detect, mean time to contain, and transaction speed.

II. ANTICIPATED COOPERATIVE COLLISION AVOIDANCE

The ubiquitous nature of Vehicle-to-everything (V2X) connectivity not only allows situational awareness of the driving conditions in advance (e.g., range of kms) but also enables the collaboration among vehicles by mutual sharing of event information, such as in ACCA. Figure 1 shows the deployed scenario, where a Network Slice is composed by C-ITS services: 2 equal NSs deployed each one into a Road-Side Unit (RSU), and the third NS in a Central Node to either share the information with other domains or other statistics actions. The threat appears when a malicious vehicular node generates a false data injection attack by an authorised vehicle node, which introduces information of a fake accident (red vehicle) that will cause traffic problems on the surrounding vehicles slowing down their speed and also to those vehicles far away which will choose a different road to avoid the accident.
This demo will focus on the management of an E2E Network Slice composed by secured and verified NSs and their Virtual Network Functions (VNFs). SSLAs will be used to identify the non-legitimate information generated by the malicious node and apply the correct solution (e.g., firewall or other options). In the cloud data centre (DC), the deployed functionalities are the management of the data generated by all vehicular Mobile Edge Computing (MEC) nodes (i.e., analytic, forwarding, etc.) through the use of a V2X communications application and the detection of malicious data generators, such as the fake vehicle accident in this demo, using an Intrusion Detection System (IDS). In the vehicular MEC, a V2X communications application is run in order to communicate with the vehicles and the cloud DC. In addition, a firewall will also be used in order to filter the traffic that the cloud DC will classify as non-acceptable.

III. DEMONSTRATION AND RELEVANCE

In order to better understand how this demonstration works, Figure 2 illustrates how each of the elements within the High Level Architecture (HLA) for secure network slicing participates in the deployment of an E2E Network Slice.

First, (1) Vertical (or Over-The-Top, OTT) requests an E2E Slice with an associated SSLA to the E2E Network Slice Manager (E2E Slicer). The E2E Slicer allocates the V2X communications application as a Network Service (NS) to the correct domain and requests its deployment to the specific Domain Slicer (Step 2). Then, E2E Slicer requests the SDN Controller to configure the inter-domain paths between NSs (Step 3). The E2E Slicer requests the associated SSLA to the E2E Policy and SSLA (PS) (Step 4). Then, in Step 5, the E2E PS requests to each domain’s PS Manager to configure and associate the SSLA to the deployed NSs. The E2E Slicer requests to the E2E Security Orchestrator (SO) the Security Functions (SF) deployment next to the E2E Slice NSs to add the expected security (Step 6), so IDS is orchestrated. The E2E SO requests to each domains’ SO the specific SF deployment (Step 7). The E2E SO requests the E2E Security Intelligence Engine (SIE) to monitor the E2E Slice (Step 8). The E2E SIE configures each domain’s SIE to monitor the NSs security performance (Step 9). Finally, once all the elements are deployed, the data is saved (Step 10), and monitoring phase starts. Once IDS detects vehicle message intrusion, it triggers the necessary actions, which result in the blocking of the non-legitimate vehicle information in the firewall.

In order to evaluate and ensure that the security functions work accordingly to the expectations and have a good performance, the demo measures the mean time to detect, mean time to contain, and transaction speed, among other metrics.

IV. CONCLUSION

We have presented a demo that provides Security SLA in V2X network slices. In an ACCA scenario, we have detected malicious vehicle data and resolved the identified threat.

ACKNOWLEDGMENT

Work partially funded by the EC 5GPPP INSPIRE-5GPlus (871808) and MINECO AURORAS (RTI2018-099178-B-I00).

REFERENCES

[1] V. Casola et al., “Sla-based secure cloud application development: The specs framework,” in SYNASC, 2015.
[2] P. Alemany et al., “Transport network slices with security service level agreements,” in proceedings of ICTON, 2020.
[3] A. Festag, “Cooperative intelligent transport systems standards in europe,” IEEE communications magazine, vol. 52, no. 12, pp. 166–172, 2014.
[4] F. Vázquez-Gallego et al., “A mobile edge computing-based collision avoidance system for future vehicular networks,” in INFOCOM 2019.
[5] R. Vidalta et al., “Vehicular message exchange in cross-border scenarios using public cloud infrastructure,” in IEEE 5G World Forum, 2020.