SC26 Network Research Exhibition: Demonstration Publishable Abstract

Trusted Remote Embassy: Kubernetes-native deployment of secure network services

Chrysa Papagianni, Cees de Laat, University of Amsterdam,
{c.papagianni, delaat}@uva.nl

Abstract

This demo showcases a Remote Embassy: a trusted network node deployed on infrastructure outside the home organization's administrative control. The setup will consist of a K8S cluster distributed across two or more sites where one is named the home organistation and manages the remote deployments through a trusted, quantum proof communication channel. The K8s cluster hosts applications and orchestrates virtual and physical network functions as service function chains, to support a variety of use cases were applications need to be distributed also outside the home perimeter but need to remain under the control of the home organisation.

To protect communication between sites, we deploy the Fortaegis F1NE devices as physical network functions. Each device incorporates an intrinsic hardware security module (iHSM) that derives its identity from a physically unclonable function (PUF): a circuit that uses physical variations introduced during manufacturing to generate a device-specific identity. The devices authenticate each other and encrypt selected traffic exchanged between sites, at high speed.

Loom is a K8s-native orchestration framework for deploying and managing application workloads and network functions across heterogeneous software and hardware targets. It provides declarative abstractions for network functions, programmable software and hardware targets, and service function chains. In the demonstration, Loom orchestrates the network functions and configures a service chain that steers application traffic through them. Through a target-specific agent, F1NE's encryption and decryption functions are integrated into the service deployment, protecting traffic exchanged between sites.

Goals

This demonstration is a first step towards the Trusted Remote Embassy concept. It brings together technologies to explore how an organization can deploy and manage network services across sites (Amsterdam and at SC in the booth of CIENA) while protecting communication between them.

1. **Kubernetes-native lifecycle management of service function chains:** Demonstrate the deployment and management of an application and its associated software and physical network functions across the home and remote sites, using a declarative service definition.
2. **Hardware-rooted secure communication**: Demonstrate how F1NE devices use identities derived from physically unclonable functions to authenticate each other and establish an encrypted communication channel between the home and remote site.
3. **Integration of hardware security into service chains:** Demonstrate how hardware-based security functions can be integrated in a service chain to protect traffic across distributed sites.

Impacts

The Trusted Remote Embassy combines technologies developed in part and integrated within Future Network Services (FNS), the Dutch national R&D programme aimed at positioning the Netherlands as a global leader in the development and standardization of next generation (6G) networks up to 2030. It addresses topics such as cloud-native networking, AI-assisted orchestration management and control and secure network services. This demonstration focuses on cloud-native deployment and management of secure network services. For the science community at large and the cyberinfrastructure serving their needs this implements methods to flexibly program assets and safeguard data in multi-tenant situations.

Resources

This demonstrator will need a normal 1 gigabit link and can run on the CIENA booth #5035 uplink. This is being coordinated with Scott Kohler. No further resources are needed.

Involved Parties

- Tomas Agata, UvA, tomas@tomasagata.dev

- Paola Grosso, UvA, p.grosso@uva.nl
- Marios Avgeris, UvA, m.avgeris@uva.nl
- Gergely Pongracz, Ericsson, gergely.pongracz@ericsson.com
- Kis Dávid, ELTE, kidraai@inf.elte.hu
- Sandor Laki, ELTE, lakis@inf.elte.hu
- Marc Makkes, Fortaegis, marc.makkes@fortaegis.com
- Ignacio Alonso, Fortaegis, ignacio.alonso@fortaegis.com
- Scott Kohler, CIENA, skohlert@ciena.com
- Rod Wilson, CIENA, rwilson@ciena.com
- Marc Lyonnais, CIENA, mlyonnai@ciena.com