

# Software-defined Security for **Network Function Virtualization**

### **Context: NFV Security**

	Operating Support System/		Orchestration (NFV MANO)	
	Business Suppo	Service, VNF,	NI (Ne	FV orchestrator twork & Service)
VNEaa	e	Infrastructure Description	N. S. S.	- Or- Volm

## **Contributions:**

- **1. Network Functions Virtualization Access Control as a Service:**
- Formal high-level specification of access control requirements to be enforced

#### Author



# Manel Smine

Phd Student 3rd year



VNF: Threat analysis - Vulnerabilities in VNF softwares - Security breaches resulting from lack of interoperability Security flaw in development life cycle Security policy and regular compliance failur Insecure interfaces Data loss and information leakage Malicious insiders DoS/DDoS attacks

NFVI: Threat analysis **NFV MANO: Threat analysis** Security issues in guest VMs Attack to management and control plane - Security issues in hypervisor - Failure of troubleshooting Insecure management interfaces Security policy and regular compliance failure Compromising virtual network component Insecure interfaces Security pitfalls of OpenStack Malicious insiders Inadequate enforcement of security policie DoS/DDoS attacks Shared physical and virtual resources Malicious insiders Untrustworthy service composition Hardware attacks

**Motivation**:

Enhancing the security of NFV services by defining an optimal deployment of access control policies

# **Research Questions:**

How to deploy access control policies on NFV

- Generic: can deploy most types of access control policy such as RBAC, ABAC,...
- **Provably correct** method for transforming the high-level access control requirement towards a domain type enforcement (DTE) specification.
- Efficient enforcement method.
- 2. Exception Management:
- Efficiently enforce complex access control policies containing **exceptions** and / or conflicting rules on NFV services
- Propose a **provably correct** priority-based DTE access control model

2022

Advisors Marc-Oliver Pahl David Espes

School

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

CYBERCNI

services?

RBAC

- How to specify high-level access control requirements to be enforced over network services?
- How to transform the high level access control policy into a concrete deployable policy?
- How to efficiently manage conflicts and exceptions that may exist between different access control policies?
- How to optimally deploy of access control model on NFV services?

3. Optimal Access Control Deployment in Network Function Virtualization:

- Formal modeling that allows to model, quantify and optimize the resources consumed and the impact in terms of latency
- Correct and optimal deployment of access control policies on NFV services

## **Current Work:** dynamic

**deployment** of access control policies on NFV services

Physical topology of

the NFV service



Policy refinement

**Provably Correct**