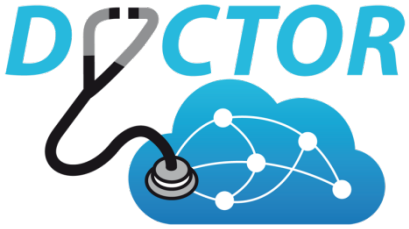


Systematic
Paris Region Systems & ICT Cluster

The DOCTOR Project

DeplOyment and seCurisaTion of new functiOnalities in virtualized networking enviRonnements

François-Xavier Aguessy – Thales

Bertrand Mathieu (Orange), Guillaume Doyen (UTT),

Olivier Bettan (Thales), Edgardo Montes De Oca (Montimage)
et Thomas Silverston (LORIA-CNRS)

21/05/2015

orange™

THALES

montimage

Loria
Laboratoire lorrain de recherche en informatique et ses applications

utt
université de technologie Troyes

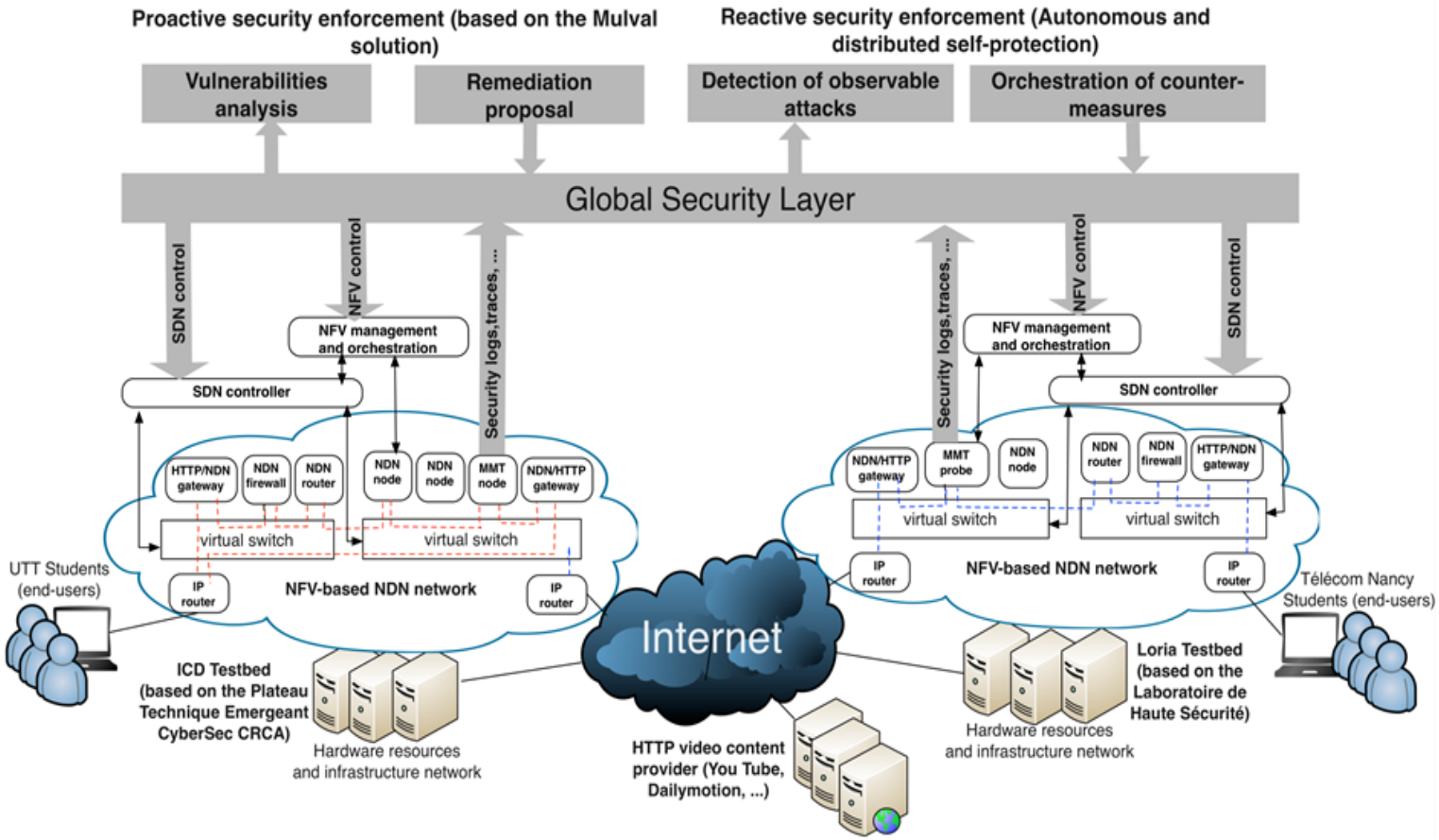
Context and Problem statement

- Deploying new network equipment is costly
- Deployment only if secure and manageable

- Cost Reduction, Hardware Mutualisation, Energy Consumption
  - Network Virtualization
  - SDN
- New networking architecture & solutions for better data delivery and optimal use of network resources
  - NDN: Named-based routing

Objectives of the project

- Deployment of new network functions and protocols in a virtualized networking environment (NDN Use case)
- Monitoring, managing and securing the virtually deployed networking architectures, using SDN for reconfiguration



Technical Locks

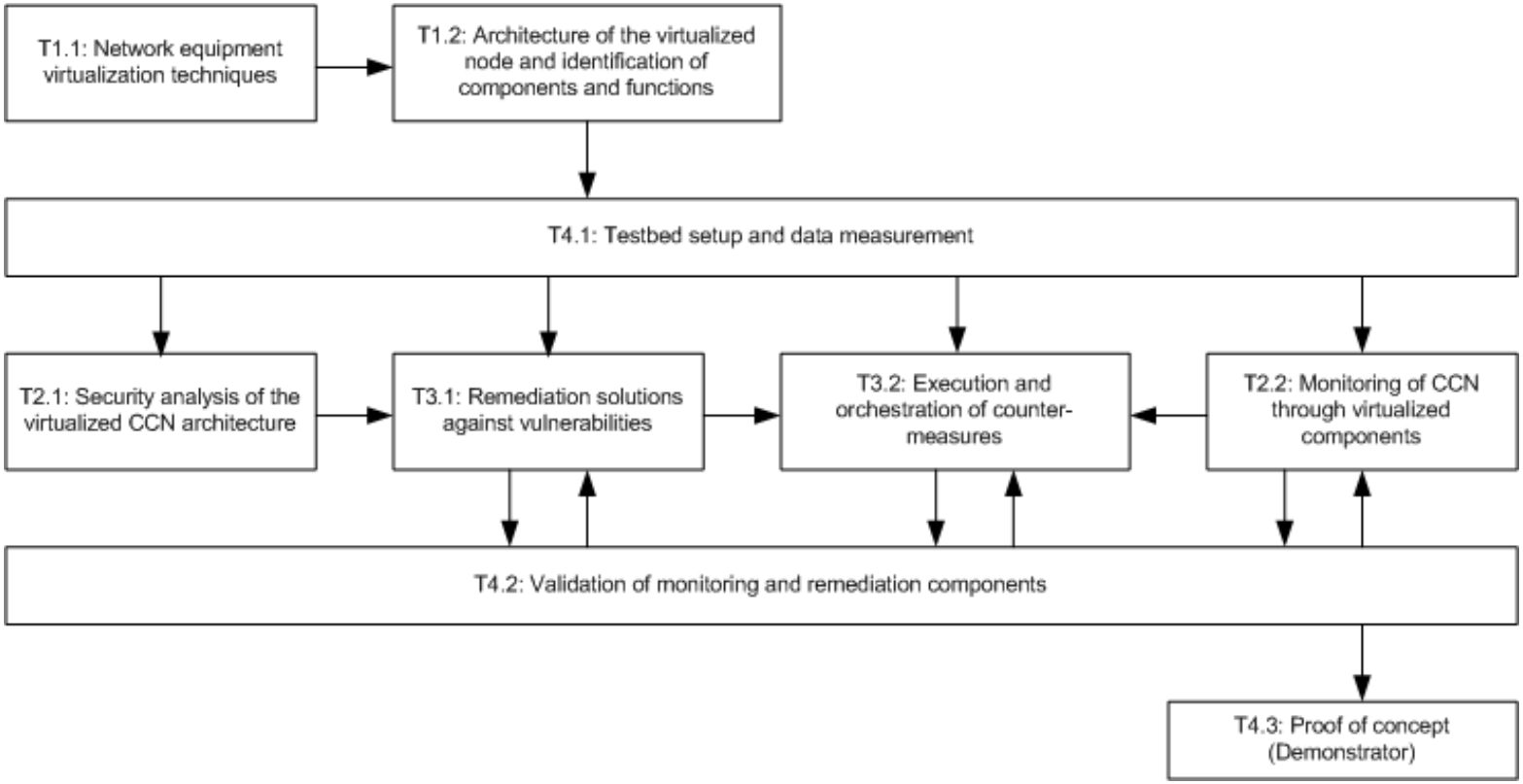
- Co-existence of multiple network protocols in the same virtualized node and migration steps
- Monitoring & Security of the virtualized NDN network: Identify flow, correlate information
- Dependability over an entire managed domain: management & control using SDN
- First testbed deploying NDN for real use: end-users accessing existing popular web sites
- Collection & Analysis of network and user data for evaluation (efficiency, performance, reliability, etc.)

Methodology

- Set up of a real testbed for end-users accessing Internet web sites
- Design and implementation of virtualized NDN network, together with a IP-based one
- Monitoring & Collection of network and usage data
- Analysis of attacks and definition of counter-measures
- Implementation of a management plane (management + security)
- Proof-of-Concept of global solution evaluated in the real testbed.

Project Organization

- Task 1: Architecture of the virtualized node for hosting network functions
- Task 2: Security analysis and monitoring of virtualized network architectures
- Task 3: Global network dependability
- Task 4: Testbed (real end-users, real services) and Demonstrator



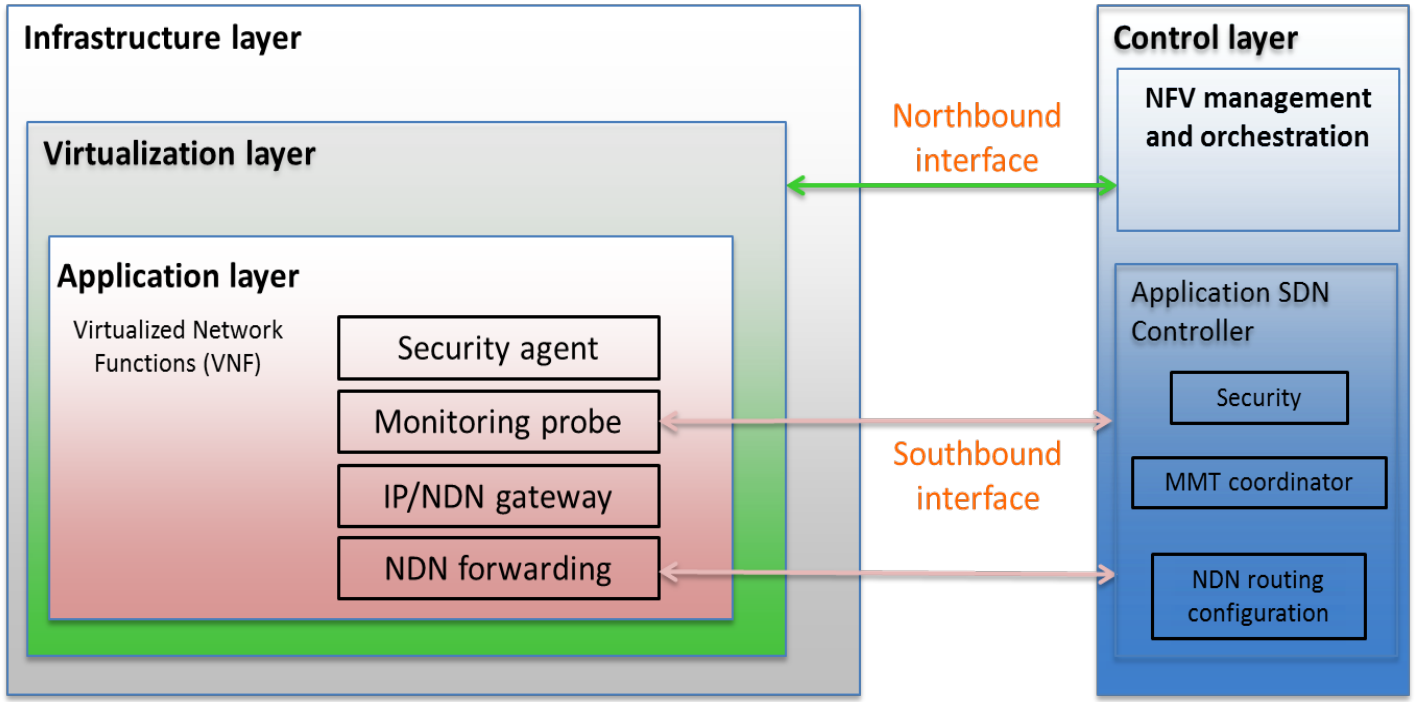
Tasks Scheduling

- T0 = 01/12/2014 Today = 21/05/2015

Id	Task/Subtask	T0	+3	+6	+9	+12	+15	+18	+21	+24	+27	+30	+33
T0	***Project management***												
T0.1	*Management*												
T0.2	*Coordination with ANR and the ongoing projects*												
T0.3	*Dissemination and Exploitation*												
T1	***Architecture of the virtualized node for hosting network functions***												
T1.1	*Network equipment virtualization techniques*												
T1.2	*Architecture of the virtualized node and identification of components and functions*												
T2	***Security analysis and monitoring of virtualized network architectures***												
T2.1	*Security analysis of the virtualized CCN architecture*												
T2.2	*Monitoring of CCN through virtualized components*												
T3	***Global network dependability***												
T3.1	*Remediation solutions against vulnerabilities*												
T3.2	*Execution and orchestration of Counter-measures*												
T4	***Testbed and Demonstrator***												
T4.1	*Testbed setup and data measurement*												
T4.2	*Validation of monitoring and remediation components*												
T4.3	*Proof of Concept (Demonstrator)*												

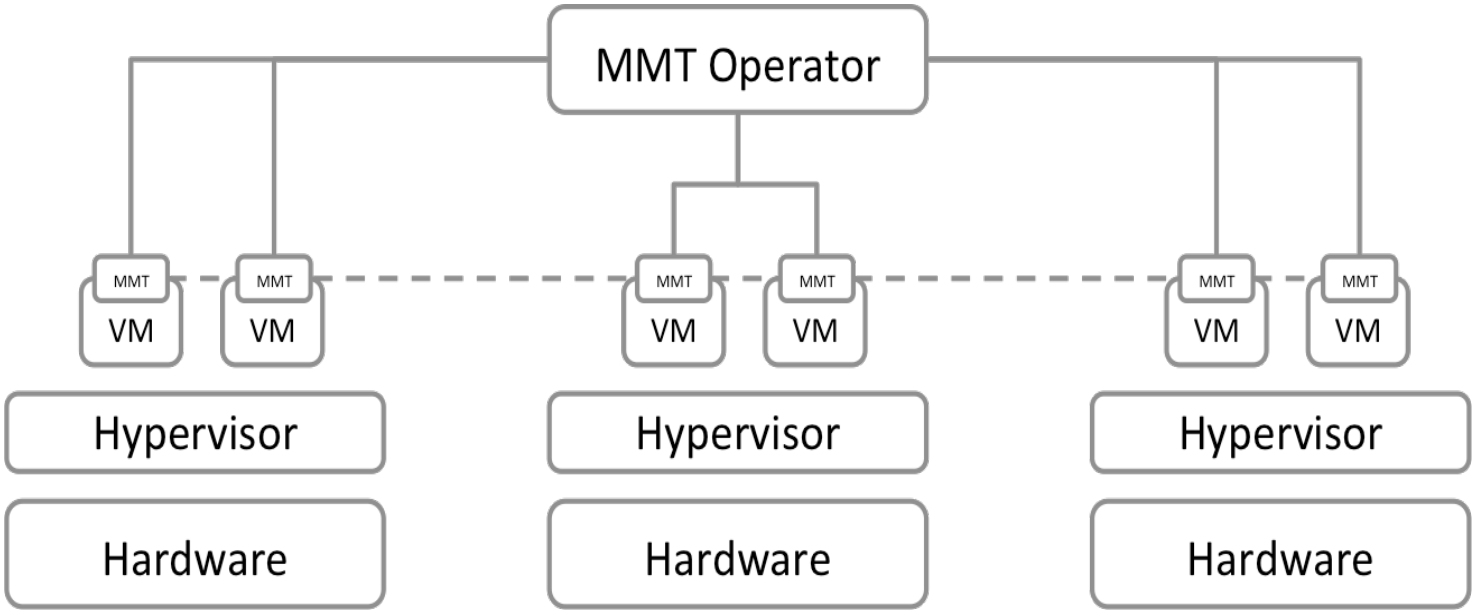
First results : Virtualization Techniques

- D1.1 : Virtualization Techniques: Analysis and Selection
  - Current virtualization techniques and their application to NFV
  - Requirements and Challenges of such architectures for DOCTOR
  - High-level architecture and candidates technologies



Monitoring architecture

- MMT probes distributed in each virtual machine.
- P2P communication, to share relevant information
- Centralized MMT Operator, for coordination and orchestration



Risk assessment and remediation

- Risk assessment based on attack graphs
- Take into account vulnerabilities specific to NDN and virtualized infrastructures
- Access to network topology and re-configuration of VFN through SDN
- Challenges of the orchestration plane
- New types of remediations, but have to take into account specificities of virtualized infrastructure

Questions

- Join us to keep updated

http://doctor-project.org/

https://twitter.com/DOCTORprojectFR

https://www.facebook.com/ProjectDoctor

https://www.linkedin.com/groups/DOCTOR-project-8240374