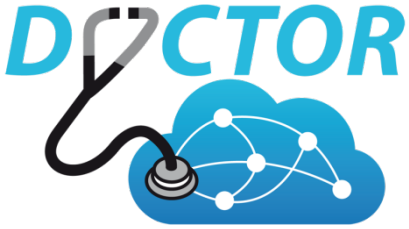


Systematic
Paris Region Systems & ICT Cluster

Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment

Bertrand Mathieu, Guillaume Doyen, Wissam Mallouli, Thomas Silverston, Olivier Bettan, François-Xavier Aguessy, Thibault Cholez, Abdelkader Lahmadi, Patrick Truong, Edgardo Montes de Oca

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 Function Virtualization
  - Software Defined Networking
- New networking architecture & solutions for better data delivery and optimal use of network resources
  - NDN : Named Data Networking
- Deployment of new network functions and protocols in a virtualized networking environment (NDN Use case)

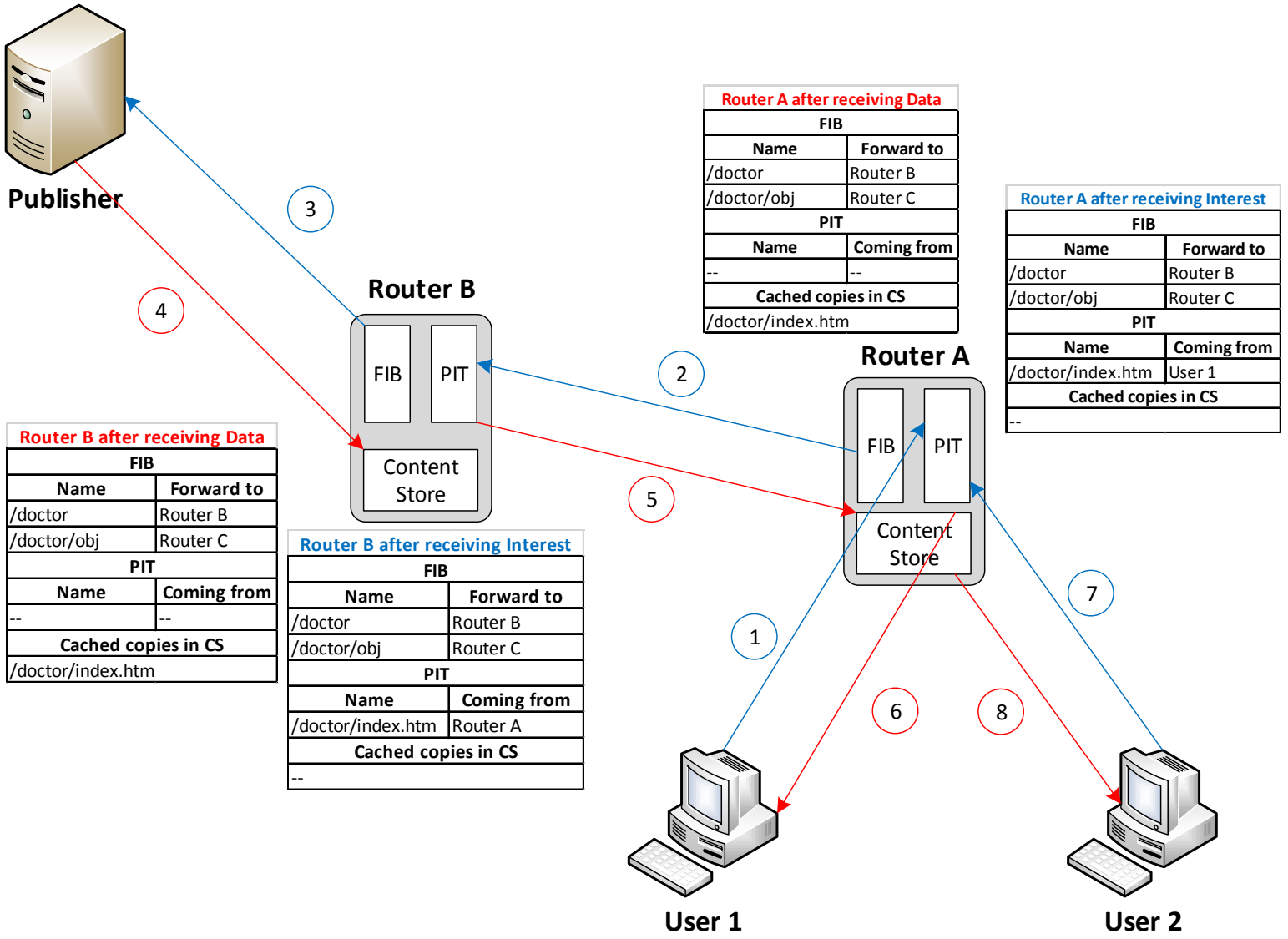
Outline

- Introduction to NDN
- Network architecture
- Monitoring solution
- Proactive and Reactive Security Mechanisms
- Conclusion and Next steps

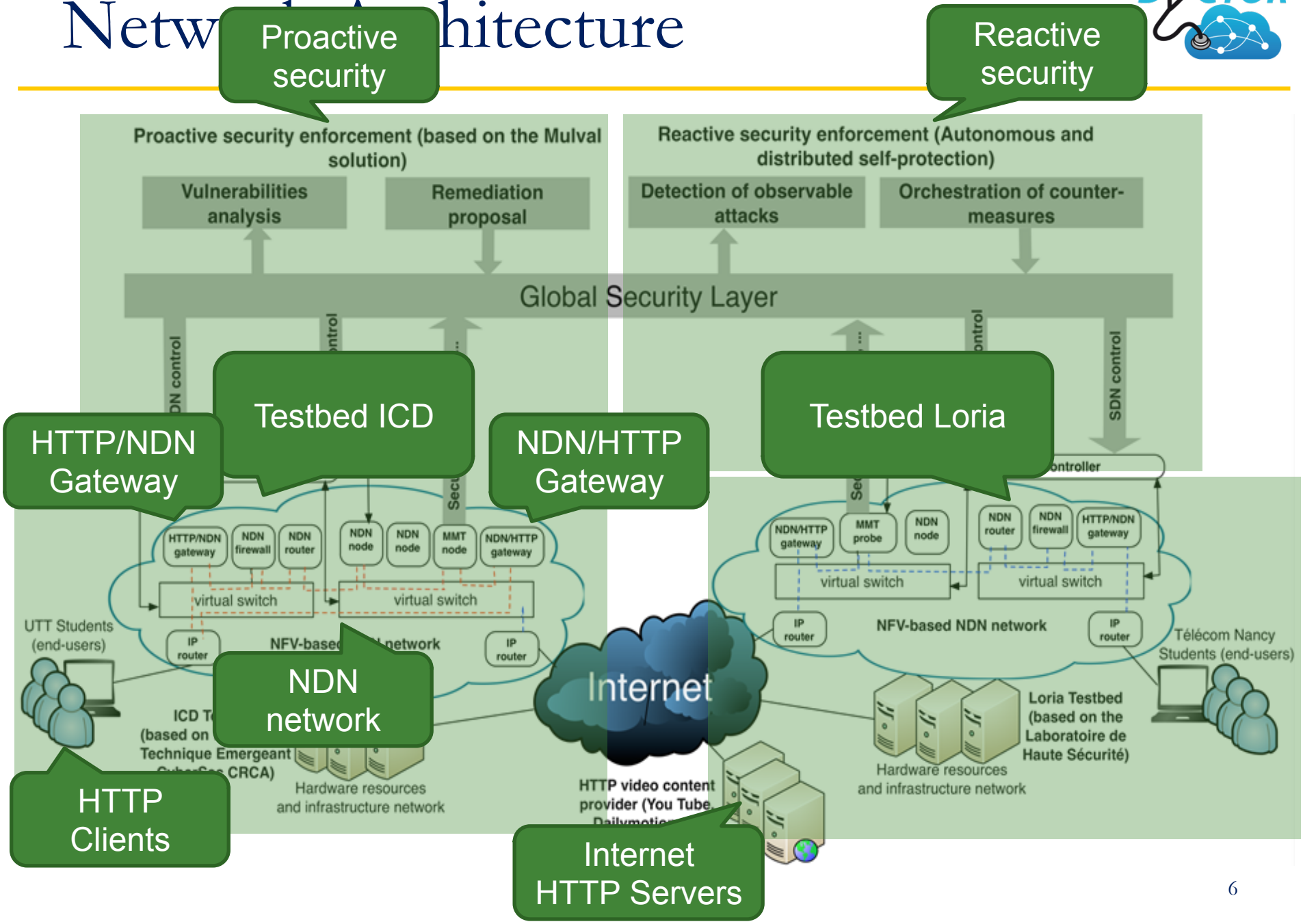
Named Data Networking

- Novel networking protocol
  - Information-Centric Networking architecture
  - Names are hierarchical
- Two types of NDN packets:
  - Interest
  - Data
- Designed for
  - Caching
  - Multicasting
  - Mobility
  - Multipath
  - Data integrity and authentication…

NDN Network exchange example

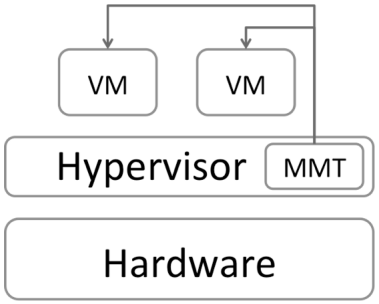


Network Architecture

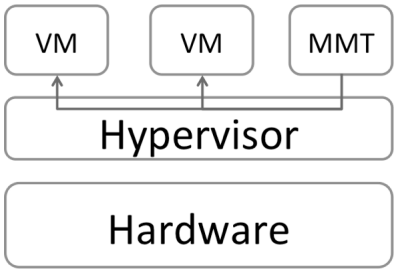


Monitoring solution

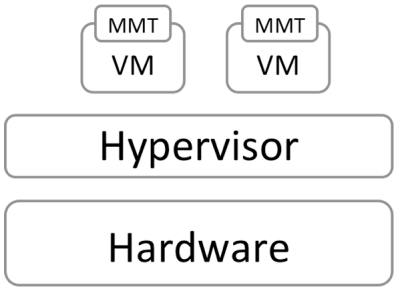
- MMT : Montimage Monitoring Tool
  - Network capture probe for traffic analysis
- 3 possibilities



Network-based



Virtual Machine introspection

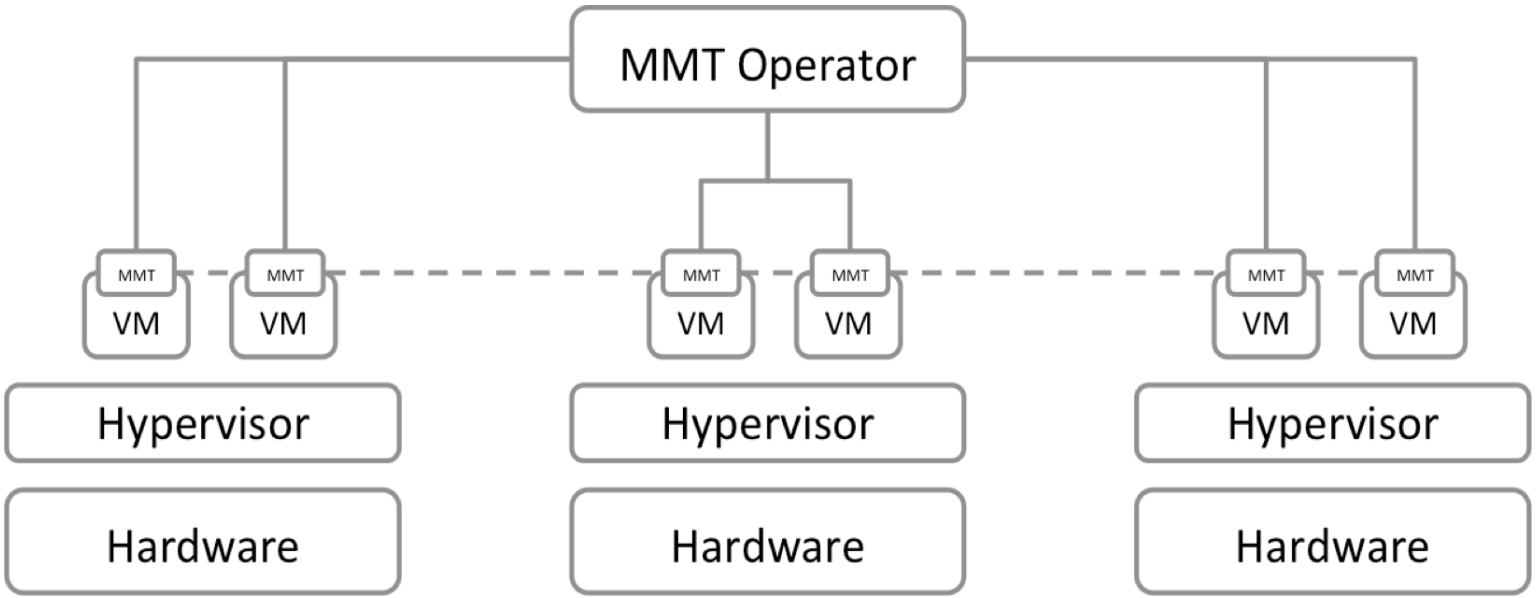


Host-based

- Host-based protection on each Virtualized Network Function
  - Better detections than network-based
  - Better performances than Virtual Machine introspection
  - Distribution of the power and memory requirements
  - Can be configured to monitor exactly what is needed for the VNF

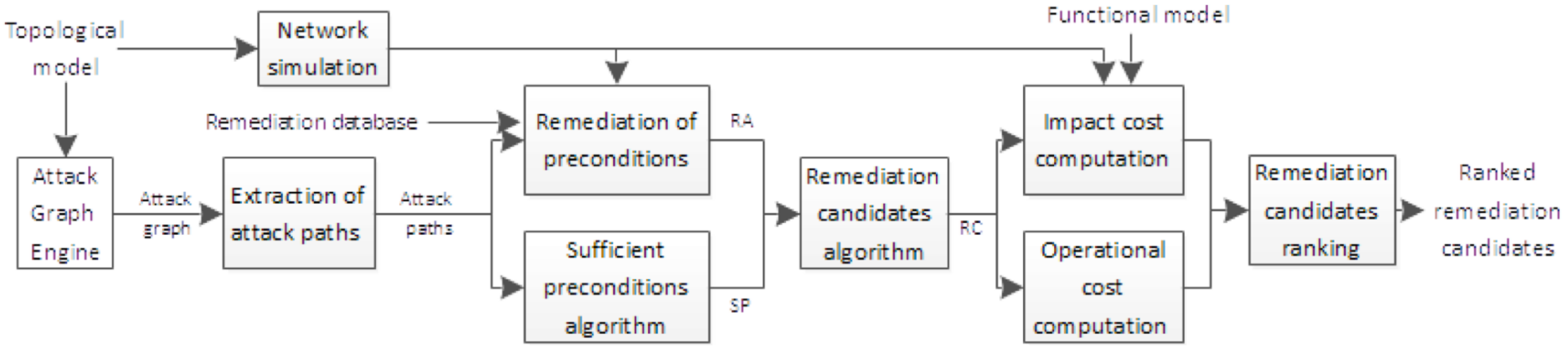
Monitoring distributed architecture

- Managed via Software Defined Networking
  - Creation of a monitoring application
  - Distributed collection of information
  - Centralized decision point (controller)
- Communication of probes via P2P for local decisions



Proactive Security Mechanisms

- Risk analysis based on attack graphs
  - Benefits from the SDN to get up-to-date topological information
  - Integration of the attacks specific to NDN (ex: cache poisoning, interest flooding attack…)
  - Describes how a localized attack can propagate in the network
- Remediation strategy



Reactive Security Mechanisms

- Generation of attack patterns from attack paths
  - To deduce the characteristics of traffic, caches or forwarding tables
  - Allow to configure the monitoring probes
- Integration of MMT with attack graphs
  - Dynamic risk assessment
  - Detections with prior-knowledge
- Countermeasures on the virtualized infrastructure
  - To stop or mitigate the currently happening attacks
  - Eg. Configure/deploy a virtualized firewall, or Intrusion Detection System

Conclusion and Next steps

- Modular monitoring architecture for virtualized infrastructure.
- Makes possible secure deployment of new protocols.
- Can be applied for migration from IP to NDN.
- Current/Future steps:
  - Implementation of the two testbeds.
  - Virtualized network functions of NDN.
  - Integration of the MMT probe into containers.
  - Evaluation on testbeds of this monitoring solution.

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