Towards Content-Oriented Orchestration for Virtual Information Centric Networking

Long HOANG MAI & Guillaume DOYEN, on behalf of the Doctor consortium

Troyes University of Technology – Charles Delaunay Institute

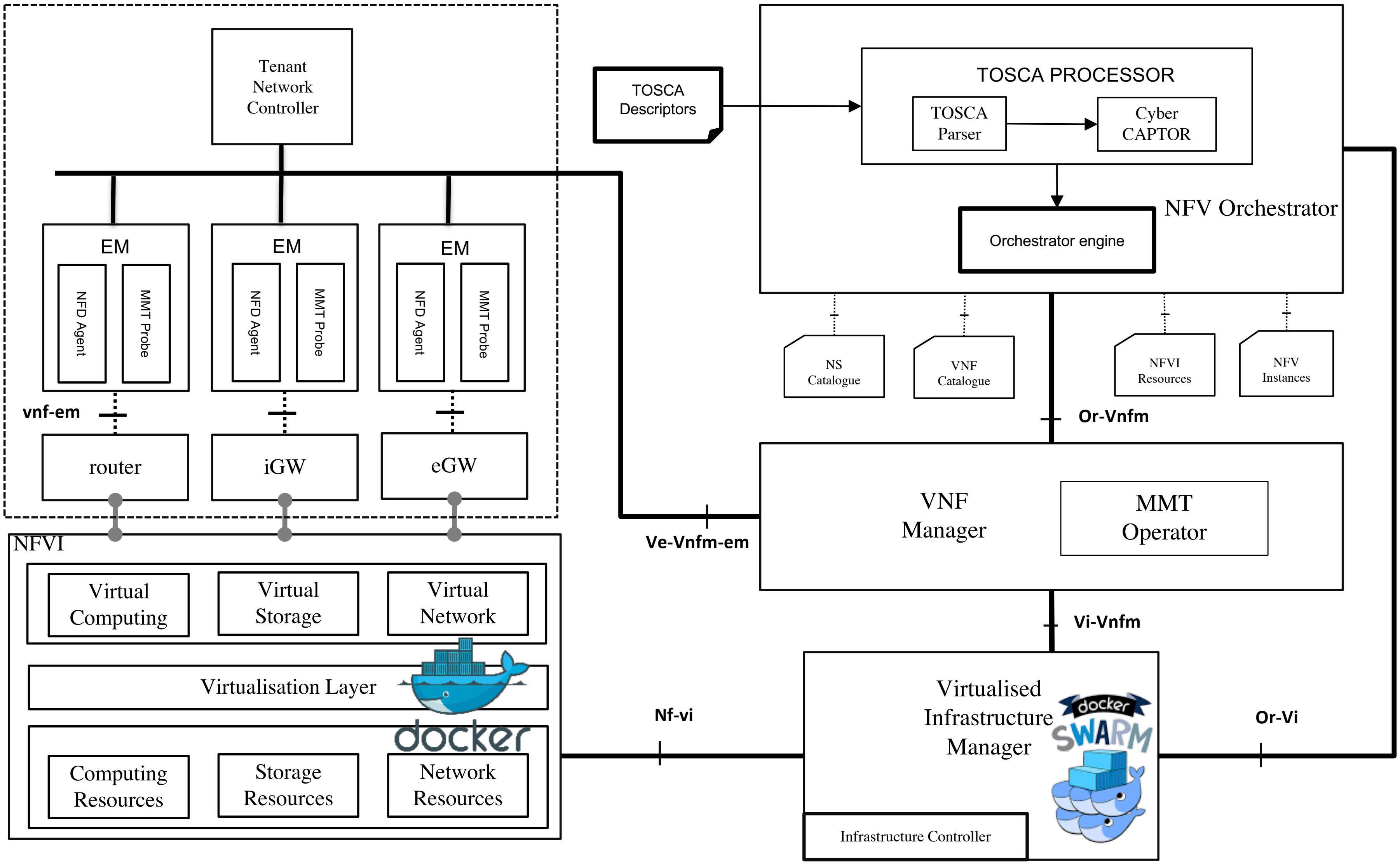
Contact : guillaume.doyen@utt.fr

ICNRG Interim Meeting (IETF #101) – London – March 18, 2018

Locks for an ICN deployment

- A pragmatic approach
  - A progressive migration performed according to opportunities
    - Services that would benefit from an ICN stack at most
    - Topological locations (access, edge, core) that best fit with ICN Traffic Engineering features (e.g. symmetric routing, caching)
  - Management and security frameworks are required
  - Cohabitation with IP can be handled through NFV
    - Isolation of network protocol stacks (keeps IP as a common substrate)
    - Cost effective solution by using commodity servers
  - This is the position of the 2014-2018 Doctor Project
    - Funded by the (French) National Research Agency (ANR)
    - Selected NDN as a target ICN technology

Content-Oriented MANO - PoC



Content-Oriented MANO - PoC

- Management
  - NDN VNF monitoring (ext. of NFD mgmt protocol)
  - Design and implementation of micro-detectors [IM 2015, WIFS 2015]
  - Event correlation [NOMS 2018]
  - A management Dashboard (partner Montimage)
- Orchestration
  - A TOSCA extension
    - Specifying an NDN service topology
    - Specifying dynamic policies
  - Implementation of a NDN orchestrator
    - A chain of MANO Components processing

A TOSCA extension for ICN (1)

- Virtual Deployment Unit
  - Abstraction describing the virtual resources over which a VNF will be executed
- Virtual Network Function
  - The piece of software that will be executed on a VDU
  - NDN router, ingress gateway, egress gateway and NDN firewall
- Virtual Link
  - Resources required to link two VDUs
- Connection Point
  - The connection capability which associates a VDU to a virtual link
- Forwarding Path and Graph
  - a list of VNFs that a particular set of NDN packets will follow
  - Uses content prefixes instead of L2/L3 flow specifications

A TOSCA extension for ICN (1)

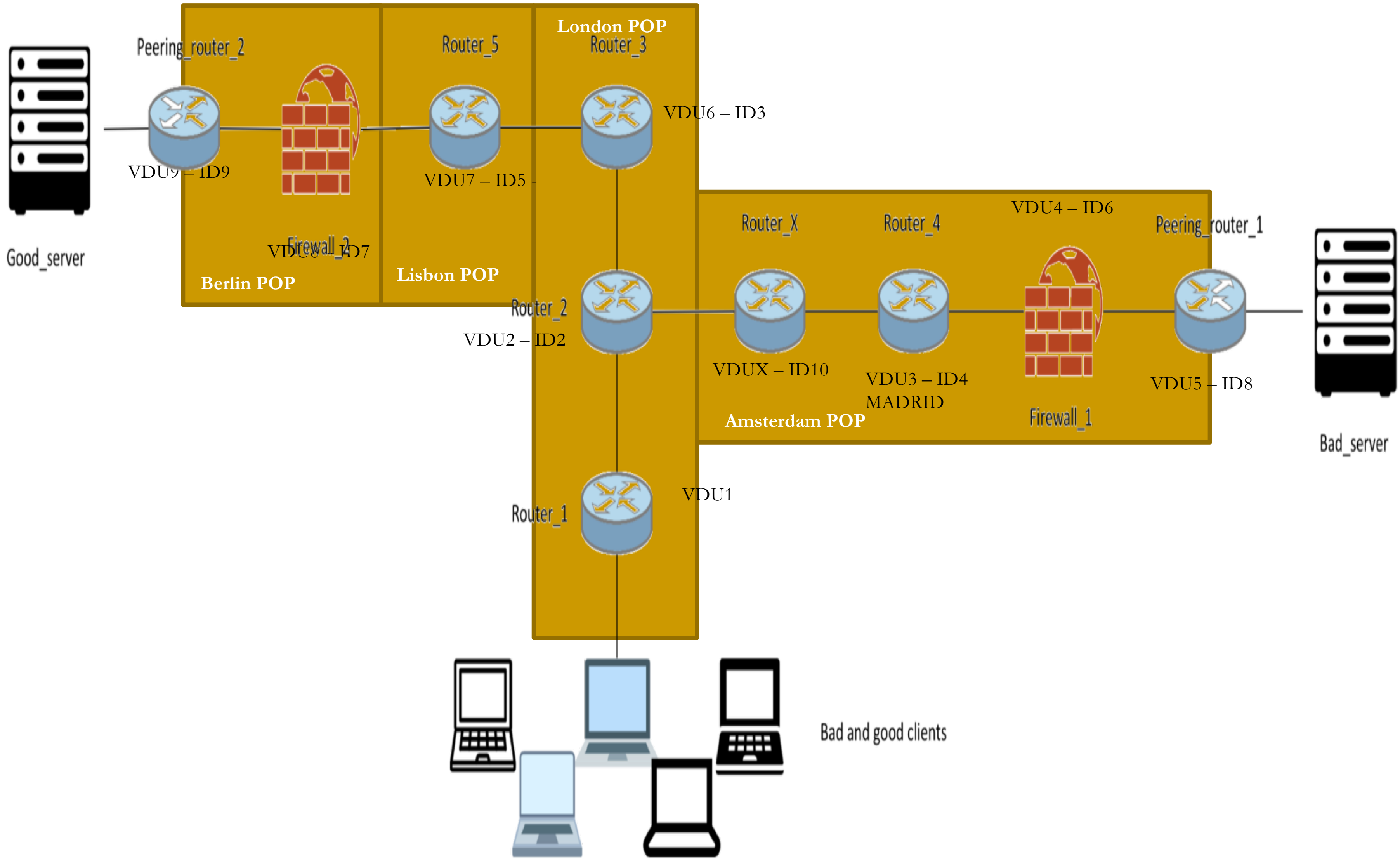
- Policies
  - Event-Condition-Action rules to apply dynamically
  - Signature verification policy: change the NDN router mode (signature verification to be applied on data packets)
  - The firewall policy: configure, at runtime, firewalls mode and configuration (i.e., white and black lists);
  - The scaling policy: monitor VNFs performance metrics and enforce a scaling-out action when a threshold is crossed

Demonstration scenario

- European telco topology
  - ClaraNet (6 PoP part of)
  - Points of Presence (PoP) made available through the Internet Zoo Topology Dataset
- Different NDN VNFs
  - NDN routers
  - Signature verification module
  - NDN Firewall
  - Ingress/egress gateways (not included)
- The whole network is deployed through virtualized means
  - 1 PoP in 1 Openstack VM
- NDN compromised server sends poisoned content
- Attack mitigation through dynamic orchestration

By claranet (claranet) [CC0], via Wikimedia Commons

Topology



Good_server
Peering_router_2
VDU9 – ID9
Firewall_2
VDU8 – ID7
Berlin POP
Router_5
VDU7 – ID5
Lisbon POP
London POP
Router_3
VDU6 – ID3
Router_2
VDU2 – ID2
Router_1
VDU1
Router_X
VDUX – ID10
Router_4
VDU3 – ID4
MADRID
VDU4 – ID6
Firewall_1
Peering_router_1
VDU5 – ID8
Amsterdam POP
Bad_server
Bad and good clients

TOSCA VNF and VDU specifications

```
router_2:
  type: tosca.nodes.nfv.doctor.VNF
  properties:
    id: 2
    vendor: orange
    version: 1.0
  requirements:
    - VDU: VDU2

firewall_1:
  type:
tosca.nodes.nfv.doctor.VNF.firewall
  properties:
    id: 6
    vendor: orange
    version: 1.0
    configuration:
      mode: accept
      rules:
        - action: append-drop
          prefix: [/foo]
  requirements:
    - VDU: VDU4
```

```
VDU2:
  type: tosca.nodes.nfv.doctor.VDU
  properties:
    name: VDU2
    sw_image: maouadj/ndn_router:v1
    config: /doctor/launch_nfd_router.sh
    flavor: medium
    placement_policy: ['popLocation==uk’]

VDU4:
  type: tosca.nodes.nfv.doctor.VDU
  properties:
    name: VDU4
    sw_image: maouadj/ndn_firewall:v1
    config: /doctor/launch_ndn_firewall.sh
    flavor: medium
    placement_policy:
['popLocation==netherlands']
```

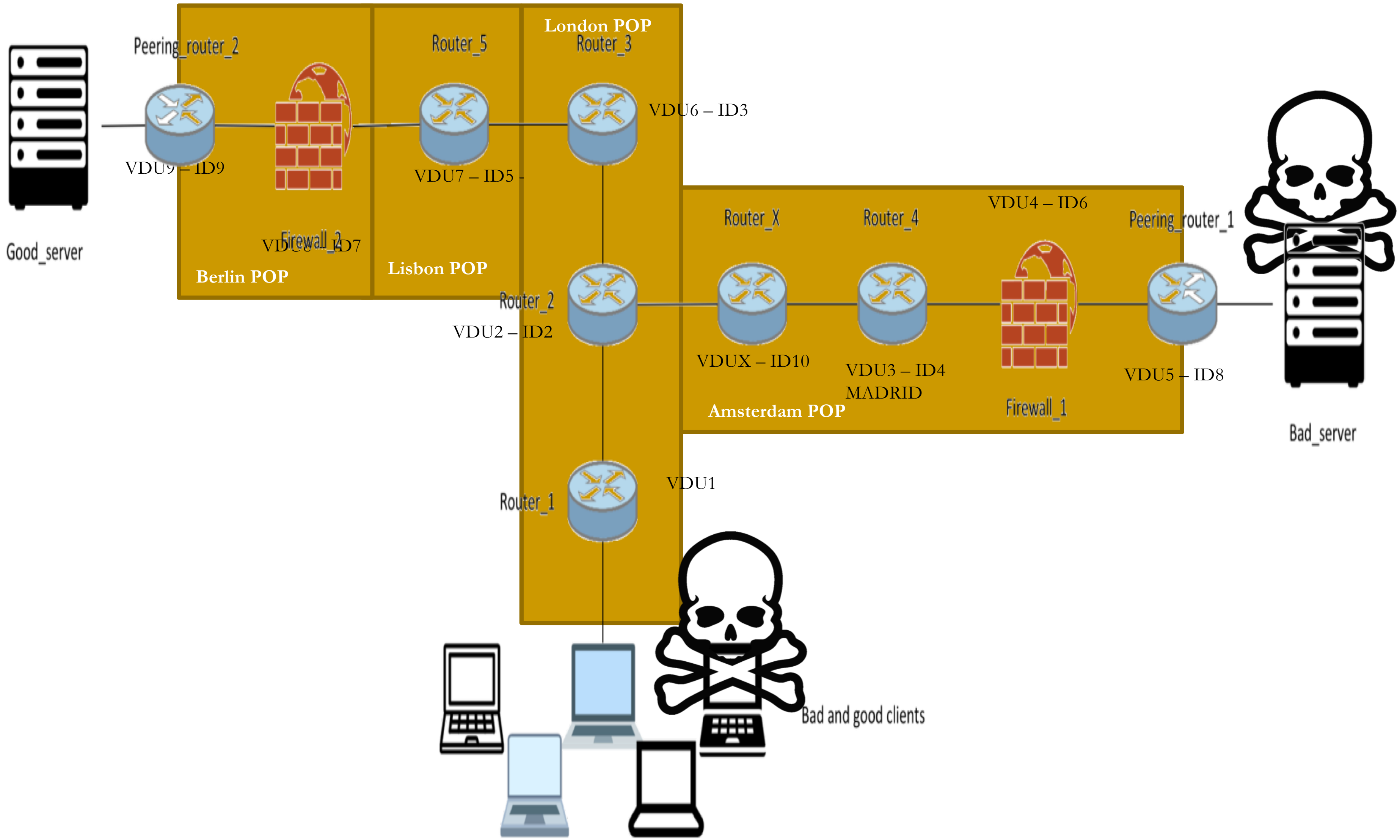
TOSCA VL and CP specifications

```
VL1:
  type: tosca.nodes.nfv.doctor.VnfVirtualLinkDesc
  properties:
    name: VL1
    connectivity_type: VXLAN

VDU1_VL1_CP:
  type: tosca.nodes.nfv.doctor.Cpd
  properties:
    name: VDU1_VL1_CP
    layer_protocol: VXLAN
  requirements:
    - virtual_link: VL1
    - virtual_binding: VDU1
```

TOSCA Forwarding Path Specification

```
http_from_r2_to_as1:
  type: tosca.nodes.nfv.doctor.FP
  description: creates path for /http
from r2 to as1
  properties:
    id: 2
    policy:
      type: NDN
      prefix: [/com/google]
      path:
        - forwarder: router_2
          capability: VDU2_VL10_CP

        - forwarder: router_x
          capability: VDUX_VL10_CP

        - forwarder: router_x
          capability: VDUX_VL2_CP

        - forwarder: router_4
          capability: VDU3_VL2_CP

        - forwarder: router_4
          capability: VDU3_VL3_CP

        - forwarder: firewall_1
          capability: VDU4_VL3_CP

        - forwarder: firewall_1
          capability: VDU4_VL4_CP

        - forwarder: peering_router_1
          capability: VDU5_VL4_CP
```

Dynamic orchestration for CPA mitigation



Content Poisoning Attack scenario

- Legitimate user
  - Requests content among 1 million whose popularity follows zifp law
  - Average rate of 10 Interests/s following a Poisson law
- Attacker consumer
  - Send Interests for popular contents
  - Top most 1% (10 000 contents) at the 64 Interests/s fixed rate
- Network
  - Setup with a multicast routing strategy
  - Do not enforce signature verification for performance purposes
- Attacker provider
  - Pushes poisoned Data to routers
- Legitimate user
  - Detects invalid signatures and asks for newer version of the same content
  - Competes with the attacker client

TOSCA policies specifications

- Dynamically starts the signature verification enforcement if a CPA alert is raised

```
policies:
  - CPA_countermeasure:
    type: tosca.policies.nfv.doctor.security.signature_verification
    targets: [router_4, router_5]
    triggers:

      peeringPoint1_verification:
        event_type: tosca.nfv.doctor.security.alert.cpa
        condition:
          constraint: triggred_by router_2
        action:
          action_type: update_router_mode
          mode: signing
          target_router: router_4
```

TOSCA Policies Specification

- Dynamically updates the firewall black list with prefixes whose signature is invalid

```
policies:
  - update_firewall:
    type: tosca.policies.nfv.doctor.ndn.security.update_firewall
    targets: [firewall_1, firewall_2]
    triggers:

    peering_point_1:
      event_type: tosca.nfv.doctor.security.alert.poisoned_content
      condition:
        constraint: triggred_by router_4
      action:
        action_type: update_firewall
        target_firewall: firewall_1
```

TOSCA Policies Specification

- Dynamically spawn NDN routers to cope with the resource exhaustion due to signature verification

```
policies:
  - scaling_out_policy:
    type: tosca.policies.nfv.doctor.ndn.scaling
    targets: [router_4, router_5]
    triggers:
      scale_out:
        meter_name: PIT
        event_type: tosca.policies.nfv.doctor.ndn.utilization
        condition:
          constraint: pending_interests greater_than 10
          threshold: 10
          comparison_operator: gt
          period: 10
      action:
        action_type: scale_out
        number: 3
```

Outline

- Context
  - On the maturity of the ICN paradigm
  - Locks for an ICN deployment
- On the road for an ICN deployment
  - Service migration
  - Management and security
  - Infrastructure means
- Leveraging NFV as an ICN enabler
  - Opportunities and challenges
  - Proposition of a Network Function Virtualization Infrastructure
  - ICN Management and Orchestration
- Demonstration
- Conclusion and perspectives

Conclusion and perspectives

- An ongoing work toward the design and implementation of NFV-MANO components for NFV
  - A proof of concept of the whole architecture
  - Code availability
    - https://github.com/DOCTOR-ANR
- Doctor and ICNRG
  - Doctor is open to serve ICNRG efforts to push forward the deployment and standardization of this network paradigm
- Future work
  - Evaluate the benefits of an NDN virtual network carrying web traffic with real end-users
  - Further explore the content orchestration
  - Explore micro-services orchestration for NDN

Questions ?

References

1. M. Vahlenkamp, F. Schneider, D. Kutscher and J. Seedorf, "Enabling Information Centric Networking in IP Networks Using SDN," *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Trento, 2013, pp. 1-6.
2. S. Salsano, N. Blefari-Melazzi, A. Detti, G. Morabito, L. Veltri, "Information centric networking over SDN and OpenFlow: Architectural aspects and experiments on the OFELIA testbed", Computer Networks, Volume 57, Issue 16, 13 November 2013, Pages 3207-3221, ISSN 1389-1286
3. N. L. M. van Adrichem and F. A. Kuipers, "NDNFlow: Software-defined Named Data Networking," *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*, London, 2015, pp. 1-5.
4. X. N. Nguyen, D. Saucez and T. Turletti, "Efficient caching in content-centric networks using OpenFlow," *INFOCOM, 2013 Proceedings IEEE*, Turin, 2013, pp. 1-2.
5. Peyman TalebiFard, Ravishankar Ravindran, Asit Chakraborti, Jianli Pan, Anu Mercian, Guoqiang Wang, Victor C.M. Leung, "An Information Centric Networking approach towards contextualized edge service," *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2015, pp. 250-255.
6. Pedro Henrique V. Guimaraes, Lyno Henrique G. Ferraz, Joao Vitor Torres, Diogo M. F. Mattos, Andres F. Murillo P., Martin E. Andreoni L., Igor D. Alvarenga, Claudia S. C. Rodrigues, Otto Carlos M. B. Duarte, “Experimenting Content-Centric Networks in the Future Internet Testbed Environment”, ICC 2013 Workshops, IEEE, 2013.
7. Salvatore Signorello, Radu State, Jérôme François, Olivier Festor:NDN.p4: Programming information-centric data-planes. NetSoft 2016: 384-389

Related Project publications

[NOMS 2018] Hoang Long Mai, Tan Nguyen, Guillaume Doyen, Rémi Cogranne, Wissam Mallouli, Edgardo Montes de Oca, Olivier Festor. Towards a Security Monitoring Plane for Named Data Networking and its Application against Content Poisoning Attack. To appear in NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium

[IM 2017] Tan N. Nguyen, Xavier Marchal, Guillaume Doyen, Thibault Cholez, Rémi Cogranne. Content Poisoning in Named Data Networking: Comprehensive characterization of real deployment. IM 2017: 72-80

[ICN 2016] Xavier Marchal, Moustapha El Aoun, Bertrand Mathieu, Wissam Mallouli, Thibault Cholez, Guillaume Doyen, Patrick Truong, Alain Ploix, Edgardo Montes de Oca. A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway. ICN 2016: 225-226

[IM 2015] Tan N. Nguyen, Rémi Cogranne, Guillaume Doyen. An optimal statistical test for robust detection against interest flooding attacks in CCN. IM 2015: 252-260

[WIFS 2015] Tan N. Nguyen, Rémi Cogranne, Guillaume Doyen, Florent Retraint:Detection of interest flooding attacks in Named Data Networking using hypothesis testing. WIFS 2015: 1-6