The DOCTOR Project
Deployment and securisation of new functionalities in virtualized networking environments

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

The DOCTOR Project
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