



Projet ANR: DOCTOR
Deployment and seCurisaTion of new functiOnalities in virtualized networking enviRonnements
Projet No.: ANR-14-CE28-0001

Compte-Rendu meeting #10  
06/04/2017  
Montimage - Paris

**Participants:**

- Orange : Bertrand Mathieu
- ICD-UTT : Guillaume Doyen, Tan Ngoc Nguyen, Messaoud Aouadj, Anis Ben Blidia
- CNRS-Loria : Thibault Cholez , Xavier Marchal, Daishi Kondo,
- Montimage : Edgardo Montes De Oca, Wissam Mallouli, Hoang Long Mai
- Thales : Théo Combe, Laurent Morel

L'agenda proposé est validé.

- **Présentation Tâche 0** : Bertrand

- **Tour de table**

Théo quitte Thales début mai, Laurent prend la suite et travaillera sur les activités relatives à la sécurité. Laurent vient de rejoindre l'équipe avec un background plus opérationnel.

Anis est un stagiaire UTT, qui travaillera pour la tâche 4.

- **Dissémination**

Le papier soumis pour un chapitre de Livre Springer, à "Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications", sur les tâches 1 & 2, a été accepté. Les principaux commentaires ont été pris en compte dans la version finale par Thales et Montimage. Une revue du papier a été faite en séance avec quelques modifications (par ex figures 2 et 3) et la version finale soumise par Théo. Félicitations à tous les



partenaires pour ce papier commun et à Théo pour avoir coordonné ce papier.

Le papier de Daishi sur « Risk Analysis of Information-Leakage through Interest Packets in NDN » a été accepté au workshop NOM à Infocom 2017. Il ira le présenter le 1<sup>er</sup> mai à Atlanta.

Montimage a participé en février au MWC (Mobile World Congress) à Barcelone et a fait des présentations en relations avec Doctor. Des contacts intéressants ont été établis.

Il est envisagé de soumettre un papier Orange/Montimage sur network slicing IP/NDN à IEEE Communication Letters.

PA Bertrand : Proposer une 1<sup>ère</sup> version et coordonner ce papier.

Il est envisagé de soumettre un papier Orange/Montimage sur le monitoring au workshop ARES/STAM.

PA Wissam : Proposer une 1<sup>ère</sup> version et coordonner ce papier.

En fonction de l'avancement des travaux et des résultats, il est envisagé de soumettre un papier commun UTT/Montimage/Loria à CNSM.

PA Messaoud & Tan : s'organiser pour le travail.

En aout aura lieu l'école d'été TAROT. Il est envisagé de faire une présentation des aspects monitoring/tests du projet Doctor.

PA Edgardo : Confirmer la possibilité de faire la présentation à TAROT et valider auprès des organisateurs.

Les journées RESSI auront lieu à Autrans (vers Grenoble) du 17 au 19 mai. Guillaume devrait y participer, au moins en partie, car en même temps que l'ETSI.

Théo a créé un espace public GitHub (<https://github.com/DOCTOR-ANR>) et un espace DockerHub (<https://hub.docker.com/u/doctoranr/>) pour Doctor. Les contributeurs intéressés du projet ont transmis leur identifiants à Théo pour être ajoutés en écriture à ces espaces.

PA ceux qui ne l'ont pas encore fait et qui le veulent : Envoyer vos identifiants à Théo pour être ajoutés comme membre des projets.

Les codes CyberCaptor et ndnperf sont déjà disponibles sur le GitHub.

Bertrand propose d'envoyer un mail à la mailing-list ICNRG pour annoncer la dispo du code ndnperf et susciter l'intérêt de la communauté pour cet outil.

PA Thibault : Envoyer mail sur liste IETF/ICNRG.

Montimage doit placer sur le GitHub le code relatif à MMT.

Pour la gateway, nous attendons les résultats d'évaluation et publication.

Nous avons aussi décidé d'y mettre les Docker File permettant de construire les containers Docker utilisés dans le projet.

Les containers complets seront aussi mis en disposition sur le Docker Hub.

PA Montimage : Mettre code MMT sur GitHub.

- **Normalisation**

Le prochain meeting IETF/ICNRG aura lieu à Prague mi juillet.

Thibault prévoit d'y aller et de présenter les avancées et résultats de la gateway.

PA Thibault : Contacter IETF ICNRG en juin pour demander un time-slot pour présenter la gateway.

Une discussion a eu lieu sur l'opportunité de présenter nos résultats sur le management/monitoring de NDN. Ce sera de nouveau discuté lors de la prochaine plénière en fonction des avancées, mais l'option actuelle est plutôt d'attendre un peu d'avoir plus de résultats de choses maîtrisées à présenter.

Guillaume s'est renseigné sur l'ETSI NFV. Il y a 7 groupes de travail dont 3 sont pertinents pour Doctor : sécurité, tests/PoC/démos et EVE sur nouveaux use-cases.

Guillaume prévoit d'aller à la réunion ETSI en mai (17-19) pour découvrir le mode de fonctionnement et les relations, avant une présentation éventuelle des travaux du projet lors d'une réunion future.

Seul problème, ce sont les mêmes dates que RESSI. Guillaume doit voir pour une organisation possible.

PA Guillaume : Coordonner participation à RESSI et ETSI.

### - **Prochaines réunions physiques**

La prochaine réunion physique aura lieu les 07 et 08 juin à Lannion, organisée par Orange.

PA Bertrand : Réserver salle de Réunion + préparer organisation

La suivante aura lieu en septembre à Paris puis la suivante en décembre à Nancy.

### • **Présentation Tâche 2** : Thibault

- Le livrable D2.2 : "Monitoring of CCN through virtualized components", est dû pour T0+30, éditeur CNRS-Loria.

Thibault coordonne la rédaction du document.

La ToC a été discutée. Il a été décidé de placer la section sur l'architecture globale du monitoring en début de document et de continuer ensuite avec son application pour les détections des différentes attaques IFA, CPA, etc.

Les sections ont été définies et chaque partenaire contributeur identifié.

Il est rappelé que toutes les activités relatives à la mitigation seront dans la tâche 3.

PA Tous : Fournir 1<sup>ère</sup> version des contributions pour le 15 mai.

PA Thibault : Coordonner contribution et intégration dans document

- Présentation Daishi : « Privacy in NDN »

Les cookies gérés par les content providers sont contre les principes de privacy.

Une étude a montré que les utilisateurs veulent mieux (et eux-mêmes) gérer leur privacy et notamment définir qui a accès à quoi.

Proposition d'avoir un network provider proxy pour gérer privacy utilisateur avec le réseau NDN et ainsi permettre aux utilisateurs un partage des infos de privacy entre les content providers et les network provider.

- Présentation Xavier : « Eclatement de NDN en 3 modules élémentaires »

Proposition d'éclatement du nœud NDN en 3 modules (PIT, FIB, CS)

Etablissement de connexions IP entre chaque modules (de 1 à N en entrée et en sortie) suivant les modules.

Dans la solution présentée, le fonctionnement de NDN est un peu modifié puisque les données (message Data) en retour passent par la FIB, qui « floode » le paquet vers tous ses clients (pas de redirection précise car la FIB n'a pas cette info).

Avoir cet éclatement permet de mettre en œuvre un réseau NDN dans l'esprit de NFV avec 3 VNFs, permettant diverses compositions/combinaisons entre les modules, et donc d'avoir au final des nœuds NDN différents. C'est plus souple que le nœud NDN monolithique. Ce n'est pas forcément l'enchaînement CS-PIT-FIB sur chacun des nœuds, mais d'autres combinaisons sont possibles (par exemple d'avoir un cache après la FIB pour tout cacher, même si pas demandé).

- Présentation Hoang : « Toward detecting IFA & CPA using MMT »

L'objectif est d'aller vers une solution plus proche de l'architecture définie en Tâche 1.

Les contrôleurs SDN et MMT security sont déployés dans le tenant, pour détecter attaques IFA et CPA directement dans le tenant. Il n'y a pas de connaissance de l'infrastructure à ce niveau.

Cette nouvelle solution permet de mettre en œuvre le contrôleur SDN distribué.

Pour l'instant, la solution détecte l'IFA, en attente pour CPA de l'algo de détection défini par l'UTT.

- Présentation Tan : « Content Poisoning Attack detection »

Etude de l'impact des attaques en fonction des composants (niveaux, client, routeurs, serveur) et en fonction des stratégies de routage (best route ou multicast).

La détection est basée sur des paramètres connus à l'avance, en fonction des estimations (statiques ou dynamiques par apprentissage).

La détection est améliorée s'il y a plusieurs points de détection sur les nœuds pour mesurer les métriques simples puis en les corrélant ensuite.

Chaque nœud monitor le nombre de « cache miss » et compare avec le nombre d'« interest » reçus par provider (vérifie si OK, sinon attaque détectée).

Cela a été implémenté avec les composants MMT probe (gestion Log) et MMT security.

- Point sur échange d'informations, notamment via le fichier XML entre Montimage et Thales

Cet échange de données est presque finalisé. Il reste quelques points à vérifier.

Montimage et Thales prévoient une réunion entre eux en avril pour clarifier les derniers points (par exemple en relation avec les CVE).

PA Montimage : Organiser une réunion dédiée.

- **Présentation Tache 3** : Guillaume

- Livrable D3.1 : " Global network reliability enhancement of virtualized network functions", dû pour mai 2017 (retardé à novembre 2017), éditeur Thales

Par manque de temps et préférant se focaliser sur le travail technique en cours pendant cette journée, ce point n'a pas été discuté.

- Présentation Messaoud : « On the control plane distribution »  
Il y a des problèmes de scalabilité des contrôleurs SDN pour gérer la connaissance de la topologie réseau.  
La solution est d'avoir 2 niveaux de contrôleur : contrôleur global et contrôleur local  
Le MMT Operator, initialement prévu dans le NFVO est plutôt localisé dans VNFM, puisqu'il gère les instances de VNFs. Dans NFVO, on retrouve Airnet (qui permet le déploiement de la topologie virtuelle en fonction des descriptions de services) et CyberCaptor.  
Pour notre use-case NDN, Airnet définit le routage entre routeurs NDN et donne la configuration à MMT operator, qui lui les enverra aux MMT Probes qui configureront le routeur NDN auxquelles elles sont associées.

Une discussion a ensuite été initiée sur la coopération entre CyberCaptor, l'orchestrateur et MMT Operator, basé sur précédentes présentations et discussions. Les rôles de chaque module s'éclaircissent et leur relation aussi. Pour avancer plus sur cette coopération, qui sera le socle de la solution Management de Doctor, une réunion dédiée sera organisée fin avril/début mai entre UTT/Thales/MMT.

PA UTT : Organiser une réunion dédiée Tâche 3

- **Présentation Tâche 4** : Wissam

- Présentation Xavier : "HTTP/NDN Gateway improvement"  
Une nouvelle convention de nommage, plus orienté NDN (suppression des identifiants de hosts) a été définie. Elle inclue aussi le protocole en préfixe (ici HTTP, mais possible d'avoir d'autres protocoles plus tard).  
Le nom de l'IGW est envoyé dans le nom NDN en format TLV pour avoir un seul composant (cela évite d'avoir un délimiteur).  
La gateway est fonctionnellement très modulaire. Par contre, à la question de savoir si ces modules pourraient devenir des VNFs dans un contexte NFV, c'est moins évident, car il y a des environnement de contexte à gérer.

Le code de cette nouvelle gateway sur le SVN Doctor.

Il faudra ensuite voir pour la dockeriser, mais ce ne devrait pas être difficile, juste quelques inclusions à faire.

PA Xavier : Fournir le Docker File pour dockeriser la gateway.

Si Thibault va à l'INCRG pour présenter cette gateway, il pourra demander si la communauté NDN prévoit de mettre en œuvre des serveurs Web NDN et voir si un tel nommage leur convient.

Montimage doit mettre à jour le parser NDN dans l'outil MMT, pour pouvoir analyser ces nouveaux noms pour affichage sur le dashboard.

PA Montimage : Mettre à jour parser NDN.

- Discussion sur spécification/rédaction d'un cahier de tests  
Il faut rédiger un document commun avec les objectifs de tests. Ce document sera ensuite intégré dans le livrable D4.3.  
Ce document contiendra la description des tests : avec/sans utilisateurs réels (injecteurs de tests comme le scrapper, nous en tant que clients, ou étudiants à la fin), les configurations réseaux à définir, avec la gateway en élément unitaire puis en tant que VNF de l'environnement virtualisé, etc.

Il est décidé de présenter chaque test avec un template incluant la description du test, l'objectif, la configuration, les paramètres d'entrée, les métriques à mesurer, la topologie réseau, etc.

Wissam fournit une 1<sup>ère</sup> version du document, chaque partenaire ajoutera ensuite les tests auxquels il pense. Il faut une 1<sup>ère</sup> version finalisée du cahier de test (pour les tests de la 1<sup>ère</sup> phase) pour le 27/04, pour qu'Anis puisse passer les tests rapidement (début mai).

PA Wissam : Fournir 1<sup>ère</sup> version du cahier de tests.

PA Tous : Compléter le document pour le 27/04.