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

Compte-Rendu meeting #7
15-16/06/2016
Orange - Lannion

Participants:

- Orange : Bertrand Mathieu, Patrick Truong
- ICD-UTT : Guillaume Doyen, Moustapha El Aoun
- CNRS-Loria : Thibault Cholez , Xavier Marchal
- Montimage : Edgardo Montes De Oca, Wissam Mallouli, Luong Nguyen
- Thales : Théo Combe

L'agenda proposé est validé.

- **Présentation Tache 0** : Bertrand

- **Dissémination**

Un papier sur NDNPerf, soumis à ICN, a été accepté. Le Loria ira le présenter.
Un papier commun UTT/Loria sur les attaques de type content poisoning a été soumis à CNSM.
Un papier commun IEEE Communication magazine, basé sur les travaux de la tâche 1, est en cours de finalisation.
Il est prévu de soumettre un papier journal commun sur le testbed, la gateway et ses performances.
Un papier UTT/Loria sur la détection des attaques de type content poisoning est prévu pour être soumis à IM.
Deux propositions de démo peuvent être soumises à ICN : une sur les attaques de type « unsoliticited provider » et une sur la démo globale avec gateway, monitoring, générateur et serveur Web en NDN natif.
Orange a soumis une proposition de démo avec gateway et monitoring au salon de la recherche Orange, l'évènement annuel d'Orange pour présenter les avancées de ses travaux.

- **Standardisation**

Thibault devrait participer au prochain meeting ICNRG, colocalisé avec la conférence ICN, et pourrait présenter les avancées du projet Doctor (notamment en relation avec

la gateway et le testbed, qui avaient été bien reçus lors de sa précédente présentation).
PA Thibault : s'enregistrer pour le meeting ICNRG
PA Tous : Préparer une présentation

- **Prochaines réunions physiques**

La prochaine réunion physique aura lieu le 20 septembre à Paris, hébergé par Thales.
PA Théo : Réservation d'une salle à cette date + organisation

La réunion ANR de mi-projet aura lieu le lundi 3 octobre à Paris à 13h30.

La réunion de projet #9 aura lieu les 17-18 janvier à Troyes.

- **Présentation Tache 2** : Thibault

Tan a fait une présentation sur le phénomène de pollution dans un réseau NDN. Il a notamment adressé la partie caractérisation des attaques de type pollution, en présentant les différents modèles et architectures. Cette étude sera utile pour sélectionner un type d'attaque et réfléchir à des solutions de remédiations. Ces travaux sont finalisés et ont fait l'objet d'un papier soumis à CNSM.

Théo a présenté un scénario d'attaque dans lequel un conteneur Docker malicieux s'échappe de son isolation pour aller lire/altérer les données des autres containers qui sont actifs sur le même host. Cette attaque est possible avec Docker grâce notamment à une faille dans l'espace de nommage et une opération de montage qui permet d'accéder au répertoire racine de la machine et non du container.
Cette attaque est maintenant corrigé par Docker mais illustre des attaques potentielles mixant les environnements virtualisés et le système. Cependant, les mises-à-jours n'étant pas automatiques et globales, ce type d'attaques est un exemple de ce que CypberCaptor pourrait détecter et pour laquelle il proposait une remédiation.
Cette présentation a aussi permis de soulever de nouveau l'orientation du projet, à savoir une solution de type Cloud privé ou cloud ouvert. Les 2 seront certainement à étudier, mais avec des orientations et choix architecturaux et technologiques peut-être différents.

Wissam a présenté les nouveautés de l'outil MMT, notamment l'intégration de l'analyse complète du protocole NDN, et des paquets NDN transportant des informations HTTP, en relation avec les conversions réalisées par les passerelles HTTP/NDN. L'outil peut maintenant très bien s'intégrer dans le testbed Doctor et mesurer, analyser, classifier le trafic NDN (avec ou sans HTTP).
MMT intègre aussi maintenant un module de détection des attaques basé sur l'algorithme IFA, proposé par l'UTT. C'est un bel exemple de collaboration entre les partenaires académiques et industriels du projet.

Nous avons échangé sur les types d'attaques mixant les technologies NFV/NDN.
Une attaque possible abordée est le remplissage artificiel de la table PIT en utilisant une faille système telle que celle décrite par Théo. Ceci permettrait de montrer qu'une faille/attaque de niveau système peut entrainer une attaque de niveau container (router NDN dans ce cas). Ce type d'attaque illustre le besoin d'un graphe d'attaques complet en ayant à la fois connaissance du tenant (container) et du système. Ceci est en rapport sur les échanges précédents relatifs au Cloud privé / ouvert. Pour ce type d'attaque, une solution avec un cas d'usage avec une isolation

pure du tenant vis-à-vis de l'infrastructure (système) n'est pas possible ou alors aura des limites en terme sécurité.
Ce type d'attaque mixte met en avant aussi le besoin d'un agent MMT sur la machine physique.
L'interaction et intégration entre les outils CyberCaptor et MMT ont été discutés. Montimage et Thales doivent faire des réunions périodiques pour définir les interfaces de communication.

Thibault a rappelé les résultats de la réunion spécifique T2/T3 qui a eu lieu à Troyes en avril, et notamment en relation avec les attaques détectables et à prendre en compte.
Le livrable D2.1 est dû pour 12/2016. Thibault a présenté l'état actuel du document qui est plutôt bien avancé, avec du contenu bien identifié. Ce livrable pourrait être disponible plus tôt que la date initialement prévu, permettant ainsi d'alimenter les réflexions de la tâche 3.
PA Thibaut + Tous : Envoyer nouvelle version du D2.1 + compléter

- **Présentation Tache 3** : Guillaume

Cette tâche étant fortement liée aux attaques identifiées dans la tâche 2, il a été choisi de sérialiser les 2 tâches, plutôt que de la faire en parallèle comme initialement prévu dans la description technique. De plus, ce sont les mêmes partenaires, donc la parallélisassion n'étant pas vraiment possible.
Cette tâche démarrera activement à la livraison du D2.1

- **Présentation Tache 4** : Wissam

Guillaume, étudiant UTT, a présenté ses travaux sur la traduction de topologies d'opérateurs de l'Internet en templates Heat d'orchestration OpenStack. Cet outil permet à partir d'une topologie réseau quelconque de construire les fichiers yaml selon le format compréhensible par Openstack. Ceci pourrait être utilisé sur le testbed si nous souhaitons émuler une topologie existante.
Moustapha a présenté les résultats des évaluations de performances de la gateway HTTP/NDN qu'il a réalisé sur le testbed de Troyes, avec ses outils (crawler + navigateurs). Ces tests sont bons puisque la gateway fonctionne très bien avec la grande majorité des sites du Top1000. Ceux qui étaient en échec l'étaient aussi avec le navigateur (indisponibles, en maintenance peut-être).
Nous avons discuté du schéma de nommage et de conversion des requêtes HTTP vers NDN. Actuellement, nous avons défini 2 schéma différents, ayant chacun ses avantages et inconvénients. Il faut aller plus loin dans l'analyse et voir lequel est le plus pertinent, performant pour notre solution.
Nous allons faire une campagne d'évaluation complète de la gateway, et notamment mesurer le nombre de requêtes simultanées qu'elle peut gérer, savoir si le point de limitation est la passerelle d'entrée ou de sortie, l'intérêt et performance des caches NDN, etc.
Cette évaluation fera l'objet d'un papier.
PA Loria : Finaliser dernière version
PA UTT : Passer les tests
PA Tous : réfléchir aux différents nommages
PA Tous : Penser à papier

Abdelhak, étudiant Orange a fait une présentation sur l'intégration des containers routeurs NDN avec OpenVswitch et illustré cela avec un scénario où un client peut

récupérer les contenus depuis les serveurs Web HTTP classiques (avec la gateway de sortie) ou directement depuis un serveur Web NDN natif (illustrant le déploiement progressif de NDN sur les serveurs Web).
Il est prévu de se mettre en relation avec Moustapha pour les containers NDN contenant le protocole NLSR.
Il faut aussi étudier la prise en compte de VxLAN entre les OVS pour avoir un réseau virtuel au-dessus des réseaux IP.
Une autre piste est aussi d'avoir les containers virtuels NDN et IP au-dessus de la couche basse de transport (Ethernet ou optique).