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

Compte-Rendu meeting #11
07-08/06/2017
Orange - Lannion

Participants:

- Orange : Bertrand Mathieu, Patrick Truong
- ICD-UTT : Guillaume Doyen, Messaoud Aouadj
- CNRS-Loria : Thibault Cholez , Xavier Marchal, Daishi Kondo
- Montimage : Wissam Mallouli, Hoang Long Mai
- Thales : Laurent Morel

L'agenda proposé est validé.

- **Présentation Tâche 0** : Bertrand

- **Dissémination**

Quelques informations ont été demandées par les éditeurs pour le chapitre de Livre Springer, à "Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications". Bertrand a envoyé les informations demandées.

UTT/Montimage/Loria vont soumettre un papier sur le détecteur CPA à CNSM.
PA UTT/Montimage/Loria : Finaliser le détecteur, évaluation et soumettre le papier

Messaoud soumettra peut-être à CNSM si les travaux sont finis. Sinon, ce sera plus tard.

L'UTT et Montimage préparent un papier journal de type TIFS (relatif aux maths appliqués pour la sécurité) sur le mécanisme de détection IFA
PA UTT/Montimage : Rédiger le papier et soumette cet été

En aout aura lieu l'école d'été TAROT. Montimage sera présent et présentera Doctor dans une session poster spécifique et fera une présentation de l'outil MMT avec un focus sur le project Doctor.
Bertrand et Guillaume ont transmis à Wissam le poster qu'ils avaient pour Doctor. Montimage pourra s'en inspirer et en reprendre des parties.
PA Montimage : Préparer poster et présentation

Le code NDNPerf est dispo sur le GitHub public. Thibault va envoyer un mail à la mailing-list ICNRG pour annoncer une nouvelle version de cet outil.
PA Thibault : Envoyer mail sur liste IETF/ICNRG.

Le code des Gateways sont sur le SVN.
Bertrand propose de faire des répertoires par démos/outils (IFA, CPA, NDNPerf, scrapper) et y placer tous les codes nécessaires (source, exe et/ou containers) ainsi qu'un manuel d'installation/opération pour installer et faire tourner la démo
PA Tous : Mettre code sur le SVN

- **Normalisation**

Le prochain meeting IETF/ICNRG aura lieu à Prague mi-juillet.
Les avancées et résultats de la gateway étant encore insuffisants, il a été décidé de ne pas les présenter à la réunion de Juillet. Il est prévu de le faire à la réunion IETF suivante.
Une discussion a eu lieu sur l'opportunité de présenter nos résultats sur le management/monitoring de NDN. De même, c'est encore un peu tôt, et nous préférerons avoir avancé sur ces réflexions avant d'y aller.

Guillaume s'est renseigné sur l'ETSI NFV. Nos travaux pourraient s'inscrire dans le groupe EVE sur les nouveaux use-cases.
Mais l'ETSI est un organisme payant dans lequel il faut venir avec une contribution identifiée et s'impliquer beaucoup pour en faire une norme. Nos travaux ne sont pas encore assez matures pour en être à ce stade.
Par contre, le groupe de travail IRTF NFVRG est plus orientée recherche et on peut y aller pour présenter les travaux Doctor. Nous prévoyons donc une présentation des travaux sur l'orchestrateur pour le meeting IETF de fin d'année.
PA UTT : En fonction de l'avancement, prendre contact avec NFVRG pour demander un slot lors de la prochaine réunion IETF pour présenter nos résultats.

- **Prochaines réunions physiques**

La prochaine réunion physique aura lieu chez Thales le 18 Septembre (date à confirmer par Orange en fonction des horaires d'avion).
PA Bertrand : Valider date de réunion
PA Laurent : Après validation, réserver salle de Réunion + préparer organisation

La réunion suivante aura lieu à Nancy les 5 et 6 Décembre avec possibilité d'assister à une seule journée pour certains et prévoir un agenda à la carte pour le 2ème jour.
PA Thibault : Réserver salle de réunion + préparer organisation

- **Présentation Tâche 2** : Thibault

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

La TOC est bien définie et les contributeurs identifiés.
Thibault attend les inputs de chaque partenaire pour le 10 Juillet au plus tard et ensuite il les agrègera et consolidera le document. L'objectif est de le finaliser avant les vacances.
Laurent voit avec Théo pour le texte des sections 2 et 4.3.
PA Tous : Fournir 1ère version des contributions pour le 10 juillet.
PA Thibault : Coordonner contribution et intégration dans document

- Présentation de Tan (UTT) sur un modèle pour détecter les attaques IFA et CPA, en fonction des métriques mesurées par les MMT probes.

Le modèle est basé sur un réseau bayésien avec apprentissage et identification des alertes qui peuvent entrainer une attaque, selon des probabilités.
Montimage (Long) va implémenter les informations à mesurer dans les sondes MMT.
Il faudra jouer des attaques IFA pour détecter le comportement et l'impact des métriques (attaques avec different payloads). Il faut aussi une réflexion sur la corrélation des données issues des nœuds.
Il a été discuté de la découpe du modèle : tout ce qui est local au nœud est dans la tâche 2, ce qui est global dans la tâche 3.
Tan et Long vont se retrouver physiquement (à Troyes ou Paris) pour travailler ensemble et avancer sur l'implémentation.

- **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

Ce document englobera la conception du système, l'identification des interfaces, la présentation de contre-mesures, les méthodes de remédiation, etc. Entre autres, nous décrirons la spécification fonctionnelle de l'orchestrateur et les relations avec autres composants (MMT Operator, MMT Probes, bus).
Après discussion sur le fonctionnement durant la réunion, nous avons convenu que le séquencement serait le suivant : MMT Operator reçoit un fichier de format Tosca d'un opérateur humain, il l'envoie à CyberCaptor pour analyse des vulnérabilités potentielles. Après réponse de CyberCaptor, MMT operator demande à l'opérateur humain de valider l'analyse fournie par CyberCaptor avec modification potentielle de la description si besoin. Puis MMT Operator fournit à l'orchestrator ce fichier Tosca « approuvé », correspondant à un déploiement possible sans vulnérabilité. Enfin l'orchestrateur se charge de deployer les composants NFV en fonction du fichier Tosca.
Le ToC du livrable D3.1 a été défini et les contributeurs identifiés.

Il est planifié de rédiger la section 2 (section de base alimentant les autres sections) pour mi-Juillet et de fournir une 1ère version des autre sections pour mi-septembre (pour pouvoir en discuter à la prochaine plénière).
PA Laurent : Envoyer à tous la ToC du D3.1
PA Tous : Contribuer aux sections

- Discussion sur contributions pour le livrable D3.2 et partage des activités entre D3.1 et D3.2

Il a été décidé que dans le D3.2 seront inclus les algos de contre-mesures, les scénarios attaques, les corrélations d'alertes, l'orchestration des micros-services et de la sécurité, l'implémentation et la validation des algos.
Une première ébauche de la ToC du D3.2 a été discutée.
Le pare-feu NDN, organe important des contre-mesures, soulève des questions. Il est prévu que le Loria le présente lors de la prochaine réunion plénière.
PA Thibault : Prévoir présentation du pare-feu NDN

- Présentation Messaoud : « Présentation de Tosca »

Tosca est un langage de description de service NFV (NFV Service Descriptor). Il permet de définir les VNFs, les virtual links, le forwarding graph, etc. et de permettre à un orchestrateur de déployer le service suivant cette description.
Il existe des librairies pour parser et vérifier la compatibilité Tosca. Cela peut être étendu avec nouvelles fonctions.
Dans Doctor, nous avons convenu d'étudier la possibilité d'étendre Tosca pour utiliser avec NDN (use-case du projet). Un des résultats du projet pourrait justement être un jeu de spécification Tosca étendu pour déployer NDN. En fonction des résultats et de l'intérêt, ces spécifications pourraient être proposées au consortium proposant Tosca.

- Présentation Long : « Decentralized MANO Cisco"

Suite à la présentation de Long, nous avons l'impression que la solution n'est pas du pur décentralisé mais plutôt un contrôleur SDN distribué
Long a présenté une modélisation des VNFs pour estimer la performance (à base de machine learning) et permettre le recherche de la meilleure chaine de VNF en fonction des performances. Ce n'est pas forcément le but de Doctor, mais serait plutôt fait dans Reflexion.
Concernant des contremesures possibles suite à une détection IFA, il a été discuté plusieurs options : isoler le trafic de l'attaquant, le diriger dans un black hole, etc. Il faut encore étudier pour peser le pour et le contre des propositions.

- **Présentation Tâche 4** : Wissam

Dans cette tâche, l'objectif est de montrer un scénario de bout-en-bout pour chacune des attaques identifiées dans la tâche 2 : IFA, CPA, Mixte.
Pour chaque attaque, il faut définir les remédiations/contre-mesures à différents niveaux et notamment celles mettant en avant et illustrant les concepts NFV.

Pour IFA, une idée est de déployer un VNF Fake server qui répond au client comme le ferait le serveur cible, mais déployé au plus proche de la eGW pour ne pas saturer le réseau. Une autre solution est d'isoler le trafic

attaquant, pour montrer qu'on peut grâce à NFV, faire des contre-mesures plus évoluées qu'avec simplement IP.

Pour CPA, 2 cas sont possibles :

- une remédiation avec déploiement d'une nouvelle version (version patch) de VNF pour l'attaque CPA de type « unsollicited data »
- une contre-mesure de type black hole (pour montrer qu'avec NFV, on peut aussi avoir les mêmes mesures qu'actuellement). L'idée est de filtrer côté interest du préfixe attaqué la face attaquant, pour les autres types d'attaques CPA

Pour l'attaque Mixte, on peut envisager une isolation de la VNF en cause et le déploiement d'une nouvelle VNF sur un serveur corrigé et redirection (chainage) du service dynamiquement. Une autre solution est la remédiation avec une mise à jour de la version Docker. Cependant, cette remédiation est plus compliquée car implique une mise à jour de l'infrastructure.

Nous avons ensuite discuté de l'expérimentation sur testbed.
Ce testbed sera utile à 2 niveaux. Pour l'évaluation des solutions de sécurité définies dans le projet : détection/réaction en environnement controlé (scrapper, tests nous-mêmes) etc. Ces tests feront l'objet du livrable D4.2.
Le testbed sera aussi utilisé pour les tests réels et les mesures de performance avec l'ouverture du testbed aux étudiants. Ces évaluations seront décrites dans le livrable D4.3.

Le livrable D4.2 est à livrer pour Mars 2018 (TO+40), comme le D3.2. Il faut maintenant définir la ToC et décrire de manière détaillée les scénarios prévus dans le projet.
PA Montimage : Rédiger ToC + Description détaillée des scénarios pour septembre