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

Compte-Rendu meeting #12
18/09/2017
Thales - Palaiseau

Participants:

- Orange : Bertrand Mathieu
- ICD-UTT : Guillaume Doyen, Messaoud Aouadj, Mustapha El Aoun
- CNRS-Loria : Thibault Cholez , Xavier Marchal, Daishi Kondo
- Montimage : Wissam Mallouli, Edgardo Montes de Oca, Hoang Long Mai
- Thales : Laurent Morel, Olivier Bettan + Anaïs et Sébastien pour la présentation

L'agenda proposé est validé.

- **Présentation Tâche 0** : Bertrand

- **Dissémination**

Un papier commun UTT/Montimage sur la corrélation d'alarmes est en cours de finalisation. Il sera soumis à NOMS, deadline le 23/09
PA UTT/Montimage : finaliser le papier
Le papier journal pour TIFS commun entre UTT/Montimage est dans une première version. Il reste les relectures finales à faire avant de le soumettre
PA UTT/Montimage : faire les dernières relectures
L'UTT envisage de soumettre un papier sur l'orchestration des VNFs avec Tosca pour NDN (Messaoud) à Netsoft : deadline en décembre
Le papier commun Montimage/Orange sur le network slicing est quasiment finalisé. Une cible possible est la session expérience à NOMS : deadline le 22/09
PA Bertrand : Finaliser papier et soumettre
Un papier sur la découpe de NDN en micros-services est envisagé : cible à définir (IFIP Networking ?) quand les travaux seront terminés

Un papier journal commun UTT/Loria/Orange sur la Gateway HTTP/NDN sera soumis lorsque les tests de la gateway auront été réalisés et analysés.
PA Mustapha/Xavier : Corriger les derniers bugs, passer les tests
PA Tous : rédiger et finaliser le papier

Le projet Doctor a été accepté pour être présenté lors de la journée valorisation organisée par l'ANR le 05/10.
Quand l'ANR aura transmis le template pour les présentations, Bertrand et Edgardo feront les slides.
Bertrand ne pouvant pas, Edgardo ira présenter le projet.
PA Bertrand/Edgardo : Faire les slides puis présenter

L'UTT (Messaoud) a fait une présentation et une démo de l'orchestrateur NDN aux journées « Cloud Days ». Les travaux ont été bien accueillis et ont suscité l'intérêt de l'audience.
L'UTT a été choisi pour organiser la prochaine édition des « Cloud Days ». Elle devrait avoir lieu avant mi-septembre 2018. Le projet Doctor sera actif dans cette organisation et pourra présenter les résultats du projet (qui sera à son terme). Il est aussi discuté d'utiliser le testbed NDN pour les participants à ces journées Cloud Days pour leur accès à Internet. Cela est une première idée et demande réflexion sur la possibilité de le faire.
PA UTT : Organiser Cloud Days 2018

- Normalisation

Le Loria ira présenter les résultats de la gateway à un meeting IETF/ICNRG après la soumission du papier sur la gateway.
PA Loria : En fonction de l'avancement, prendre contact avec ICNRG pour demander un slot lors d'une réunion IETF pour présenter nos résultats.
Lorsque une version majeure de NDN sortira, Xavier adaptera (si besoin) l'outil NDNPerf pour cette dernière version et une annonce à la communauté ICN sera faite pour faire connaître NDNPerf.
PA Loria : Annoncer NDNPerf dès que OK.

Lorsque les travaux sur l'orchestrateur seront terminés, l'UTT (Messaoud) ira les présenter à un meeting IETF/NFVRG.
PA UTT : En fonction de l'avancement, prendre contact avec NFVRG pour demander un slot lors d'une réunion IETF pour présenter les résultats.
Se posera aussi la question de les présenter à l'ETSI lors d'un workshop par exemple.

- Prochaines réunions physiques

La prochaine réunion physique 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

Il est aussi prévu d'organiser un meeting intermédiaire dédié au développement, réunissant Xavier, Mustapha, Messaoud, Long.

PA Messaoud : Organiser ce meeting de développement dès que les composants sont prêts (vers début octobre)

- **Présentation Tâche 2** : Thibault
- Le livrable D2.2 est dû pour T0+30, éditeur CNRS-Loria.

Le livrable est maintenant complet avec toutes les contributions.
Après discussion, il est décidé d'inclure un graphe d'attaque en guise d'exemple aux règles citées dans la section 2.
PA Thales : Fournir graphe d'attaque (+ lien avec montimage)
Il est aussi décider d'enrichir un peu la section 3 sur le monitoring NDN pour mieux expliquer
PA Long + Bertrand : Enrichir section monitoring
Une fois cela fait, le livrable sera quasiment finalisé, il restera les relectures finales
PA Tous : Relire le livrable

- **Présentation Tache 3** : Guillaume
- Livrable D3.1 : " Global network reliability enhancement of virtualized network functions", dû pour novembre 2017, éditeur Thales

La section 2 (UTT/Montimage) est renseignée.
L'architecture est présentée. Il est prévu d'avoir des interfaces REST sur toute l'architecture, Montimage va adapter le code de ses composants pour passer sous REST.
Le plan du livrable est rediscuté entre les partenaires et clarifié pour mieux cibler le contenu de chaque sous-section et gérer l'articulation entre le D3.1 et D3.2.
PA Montimage : Adapter code pour utiliser REST
Il faut ajouter les spécifications des interfaces ou les API dans le livrable
PA UTT/ Montimage : Ajout APIs
Les détections d'alarmes seront « poussées » vers le Dashboard MMT, qui devra donc inclure cette fonctionnalité « push », en plus du « pull » actuel
PA Montimage : Ajouter prise en compte de la fonction Push dans MT Dashboard

Pour avancer sur le développement et intégration entre les composants des partenaires, il est prévu d'organiser une réunion d'intégration avec les personnes concernées : Xavier, Mustapha, Messaoud, Long au minimum + d'autres s'ils veulent.
PA Messaoud : Organiser ce meeting de développement dès que les composants sont prêts (vers début octobre)

- Présentation Thales (Anaïs/Sébastien) : certification de fonctions virtuelles :

L'objectif de ces travaux, en lien avec les études 5G, est le déploiement de VNFs dans un environnement sécurisé. Cela passe par la certification des VNF et la sélection de VNF en fonction de critères répondant aux exigences.
Pour cela, un enabler de sécurité pour VNF a été défini. Il propose un procédé de certification, incluant un fichier de type TWProfile, décrivant 8 attributs fourni par le fournisseur de VNF, qui est utilisé pour la certification, en lien avec le fichier TOSCA qui décrit la VNF.
Les certificats générés (Hash + nom VNF signé par certifieur) sont stockés dans un serveur.

La sélection et le déploiement de VNF se fait avec Tacker et OpenStack, NFVO communique avec le DTWC repository. Le VNF Manager récupère le descripteur de VNF (fichier Tosca) et traduit en fichier HOT, format utilisé par OpenStack Heat.
Nous avons ensuite discuté de la possibilité d'intégrer ce framework de certification dans l'architecture Doctor.
Il a aussi été discuté de son intégration potentielle dans un scénario de bout-en-bout. Un exemple pourrait être le choix de la VNF adaptée si le scénario inclue un besoin de vérification des signatures des paquets dans une VNF ou pas. Ceci a entrainé les échanges sur les aspects performance vs securité.

- Présentation + Démo de Messaoud sur l'implémentation de l'orchestrateur (avec intégration de NDN dans le langage Tosca)

Un fichier Tosca décrivant les VNF, les VL et CP est utilisé pour les VNF Doctor.
Ce fichier se base sur un langage Tosca enrichi pour traiter la sémantique NDN.
Dans le fichier Tosca, pour l'instant, on définit le routage NDN entre les VNF de routage en dur, mais une évolution est en cours pour intégrer le routage avec les fonctions.
On peut aussi définir des règles, en cas d'attaques par exemple, pour proposer des réactions automatiques
Montimage pense à intégrer un éditeur Tosca dans le Dashboard MMT pour pouvoir modifier le fichier Tosca si une réaction par l'utilisateur est requise en cas de problème ou alarme.

- Présentation + Démo de Daishi sur le parefeu NDN

Le pare-feu est conçu pour être « High extensibility, high performance ».
Ce pare-feu NDN peut avoir une utilisation en réseau entreprise entre les clients et le monde extérieur.
Il a été choisi d'utiliser des Cuckoo Filter plutôt que des Bloom Filter, car ils sont optimisés et prennent moins de place.
L'inconvénient d'utiliser de tels filtres est qu'il est impossible de spécifier des « wildcard (*) » dans les règles du pare-feu. Ce point doit être investigué.
Il existe actuellement 2 méthodes (get, post) et 2 actions (accept, drop) pour configurer le pare-feu. Il a été discuté de la possibilité d'ajouter une action « redirect ». Il a aussi été mentionné d'ajouter d'autres paramètres pour les actions (e.g. meta info, freshnessperiod, etc.).
La communication pourra se faire facilement avec l'orchestrateur via JSON. L'UTT et le Loria doivent se rapprocher pour mieux définir la collaboration entre les 2 modules.
PA UTT/ Loria : Définir collaboration entre orchestrateur et pare-feu

- Présentation Long sur corrélation alarmes

Long a présenté un plan de monitorage de la sécurité NDN.
Dans ce travail, Long a identifié les métriques d'un nœud NDN pour la caractérisation des faces, du Content Store et de la PIT (la FIB n'est pas prise en compte dans le travail présenté) et leur instrumentation a été réalisée grâce à la sonde MMT.
Un micro-détecteur pour chaque métrique permet de détecter tout comportement anormal (modification de la distribution statistique d'une métrique).

Une corrélation des alarmes par un Réseau Bayesien permet d'identifier un type d'attaque particulier (ici CPA).
Enfin, la performance de la détection est validée par le biais d'expérimentations sur le testbed Doctor à l'aide du travail mené pour la reproduction réelle de l'attaque CPA (papier UTT/LORIA IM 2017).

- Présentation Tâche 4 : Wissam

- Présentation Mustapha sur les tests de la Gateway HTTP/NDN

Mustapha a fait de nombreux tests en faisant varier différents paramètres et a mesuré l'efficacité de la gateway.
Il a été vu quelques pourcentages de perte d'objets en NDN, mais en cas de retransmission pour ces contenus, il y a 100% de réussite.
Il faudrait voir si le problème est similaire avec IP (cas classique) ou pas, cela pouvant démontrer simplement des problèmes réseaux et pas forcément des gateways.
Durant les tests, un manque de fiabilité de la gateway a été détecté : il y a des crashs de temps en temps. Une réunion d'intégration et de « debugage » sera organisée le 28 et 29 Septembre dans les locaux de l'UTT. Tous les développeurs sont conviés à cette réunion (UTT/LORIA/Montimage).
L'UTT informe qu'Anis Ben Blidia quitte l'UTT en fin Septembre (fin de stage).
PA UTT : Organiser la réunion d'intégration/debug
PA Tous les développeurs : Rendre robuste la gateway et passer les tests de performance

- Livrable D4.2 : discussion sur les scénarios pour chaque attaque

Nous avons discuté de 3 scénarios de détection et de réaction relatifs aux 3 attaques définies dans le D2.2.
Pour simplifier l'implémentation, une seule topologie sera prise en compte pour les 3 scénarios (celle de l'attaque CPA car c'est la plus complexe).
Le D3.2 spécifiera théoriquement les réactions pour chaque attaque et le D4.2 les implémentera.
Des questionnements ont été émis par Montimage sur les éléments qui doivent être remontés lors d'une détection d'attaques (flux d'attaque, face, source, contenu pollué, etc.).
Les métriques à mesurer sont celles définies précédemment pour le D4.3 : taux de faux positifs/négatifs, overhead du monitoring (CPU, mémoire), temps de réaction.
PA Montimage/tous : récupérer les scénarios relatifs à la sécurité pour les mettre dans le D4.2.

- Ouverture Testbed au public : déclaration CNIL, recrutement testeurs, annonce, etc.

Une ouverture du testbed aux étudiants est envisagée vers fin Janvier 2018.
Possibilité de décaler à Février/Mars 2018 si retard.
PA UTT/Loria : Faire les démarches nécessaires en interne et externe pour cette ouverture