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

Compte-Rendu meeting #13
05-06/12/2017
Loria - Nancy

Participants:

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

L'agenda proposé est validé.

– **Présentation Tâche 0** : Bertrand

- **Dissémination**

Un papier commun UTT/Montimage sur le plan de monitoring pour la sécurité NDN a été accepté pour NOMS 2018.
Un short paper commun entre les partenaires sur la gateway HTTP/NDN sur environnement NFV a été accepté à NOMS 2018.
Un papier commun UTT/Loria/Montimage sur sécurité NDN a été soumis à un journal IEEE Comm Mag special issue sur ICN security

Un papier commun de démo sur détection/réaction CPA sera soumis à ICIN
PA Wissam : Finaliser papier
L'UTT rédige un papier sur l'orchestration de contre-mesures pour NDN, appliqué à la sécurité (CPA) pour soumettre à Netsoft : deadline 18 décembre
PA Messaoud : Finaliser papier
Un papier journal commun UTT/Loria/Orange sur la Gateway HTTP/NDN sera soumis à Elsevier Computer Networks lorsque les tests de la gateway auront été réalisés et analysés.

PA Bertrand : Tester la gateway avec l'outil d'Antoine et enrichir les évaluations (par ex découpe HTTP/HTTPS par objets, volumétrie associée, mesure de PLT, etc.)
PA Tous : rédiger et finaliser le papier
Un papier sur la découpe de NDN en micros-services est envisagé : cible à définir (IFIP Networking ?) quand les travaux seront terminés.

Le projet Doctor a été présenté (par Edgardo) lors de la journée valorisation organisée par l'ANR le 05/10.

- **Normalisation**

L'UTT et le Loria iront présenter les résultats de Doctor lors du prochain meeting IETF (ICNRG et NFVRG) à Londres (17-23 mars). Plusieurs présentations sont envisagées :

- Gateway HTTP/NDN: Xavier/Thibault
- Monitoring ICN à ICNRG: Long
- Network Monitoring Function Virtualisation à NFVRG: Long
- Orchestrateur à NFVRG et ICNRG : Messaoud/Guillaume

PA UTT/Loria : Prendre contact avec ICNRG et NFVRG pour demander des slots pour présenter les résultats.

- **Rapport ANR T0+30**

Le document a été revu tous ensemble pour valider son contenu.
Manque seulement maintenant quelques informations budgétaires de l'UTT
PA Guillaume : Envoyer à Bertrand les infos dès que possible
PA Bertrand : Envoyer à l'ANR ensuite

- **Prochaines réunions physiques**

La prochaine réunion physique aura lieu à Troyes les 13-14 mars.
PA Guillaume : Réserver salle de réunion + préparer organisation

La réunion plénière suivante aura lieu à Lannion les 12-13 Juin. Eventuellement, elle pourrait être reprogrammée à Nancy si besoin du testbed.
PA Bertrand : Réserver salle de réunion + préparer organisation

La dernière réunion aura lieu à Paris (organisée par Montimage) en fonction de la revue finale ANR (Septembre ?).
PA Bertrand : Demander à l'ANR quand pourrait avoir lieu la revue finale
PA Wissam : Réserver salle de réunion + préparer organisation ensuite

Il pourrait aussi être organisé un meeting intermédiaire dédié au développement et aux tests dans le cadre de la tâche 4. A voir si besoin ou pas.

- **Présentation Tache 3** : Guillaume

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

Il a été discuté de la figure 1 (architecture globale) et notamment les interfaces entre orchestrateur / MMT / CyberCaptor.

Il faut revoir la section 2 qui doit se focaliser uniquement l'architecture et les updates, et non pas décrire de nouveau les rôles des composants
Dans la section 3, il faut inclure la description fonctionnelle de tous les composants
La ToC a été complétée avec tous les inputs attendus et les contributeurs identifiés.
L'objectif est de finaliser ce livrable pour le 15 janvier.
PA Tous : Fournir les inputs attendus sur leurs sections
PA Laurent : Agréger et relancer si besoin

- Démo de Messaoud sur orchestrateur

La démo a bien fonctionné et illustre bien la détection d'anomalie et les remédiations mise en œuvre par l'orchestrateur (activation vérification sécurité + scale up de fonctions)
La description Tosca a été présentée mais il faut un peu mieux montrer les modifications réalisées pour prendre en compte NDN.
Il faut mettre en avant le travail effectué pour développer l'orchestrateur.
La démo est OK mais il faut revoir un peu « l'enrobage » et le discours pour avoir une démo sympa à ICIN.
Il faut y ajouter MMT pour afficher la représentation graphique de la topologie et montrer quand elle évolue (scale up avec plus d'instances) et le dashboard pour voir les alertes/attaques

Il y a eu des échanges sur Orchestrateur/Tosca et notamment sur la dynamicité de la reconfiguration (OK pour topologies, NOK pour logique de services) dans la philosophie NFV. Faut-il étendre, aller plus loin ? Comment automatiser Tosca avec des évènements inconnus ? L'idée est plutôt de son conformer à ETSI NFV et de faire un orchestrateur simple mais efficace. C'est ce qui sera soumis à Netsoft avec un orchestrateur classique pour sécurité. On pourrait ensuite éventuellement faire évoluer pour avoir un orchestrateur plus dynamique avec rechainage par exemple pour NDN avec les micro-services.

PA UTT/ Montimage : Finaliser rédaction papier démo à ICIN
PA UTT/ Montimage : Finaliser démo avec intégration de tous les composants et définir un scénario sympa

- Présentation de Daishi sur le parefeu NDN

Daishi a présenté les premiers résultats d'évaluation de performance de son pare-feu. Il a considéré comme variables, le nombre de cœurs virtuels associés au processus et la taille des préfixes (en nombre de composants). La complexité de son algorithme de lookup dans la table de règles étant O(1), il a utilisé un set fixe de 1000 règles. Les premiers résultats montrent un impact nul du nombre de coeurs et un impact très faible de la longueur des prefixes. Les résultats ont aussi montré que c'est le parsing des paquets qui est couteux en termes de temps de traitement, bien davantage que la consultation de la structure de données utilisée pour le filtrage.
PA Daishi : étendre les mesures sur des plages plus grandes (par exemple la longueur des prefixes qui ne va à ce stade que de 1 à 3), et vérifier empiriquement la complexité de la fonction de lookup.

- Présentation Long sur un réseau bayésien pour corrélation d'évènements

Long a présenté des résultats synthétiques basées sur une implémentation du réseau Bayesien de corrélation d'événements NDN pour la détection d'attaques dans les outils Montimage. Ces résultats sont intégrés dans la soumission CommMag, call ICN Security, et montrent la bonne capacité de la chaine de traitement à détecter les attaques considérées dans le projet. Par ailleurs, Long a présenté les premiers résultats du portage de ce réseau Bayesien sur NFN (Named Function Networking). Sur un rejeu d'attaque CPA, les résultats sont probant en montrant que des inférences stockées dans un cache NDN peuvent être réutilisées ultérieurement.
PA Long : Ces travaux sont embryonnaires et nécessitent davantage d'investigation sur : l'espace des variables du réseau (binomiales actuellement), la considération d'un espace de nommage adapté pour agréger des résultats et l'utilisation des champs de version pour aller vers une approche davantage séquentielle.

- Livrable D3.2 : " An orchestration plane for the self-protection of a virtualized architecture against observable attacks", dû pour mars 2018, éditeur UTT

Il a été revu l'articulation entre les livrables D3.1, D3.2 et D4.2. Le D3.1 ne contient que la spécification du plan d'orchestration. Le D3.2 les algorithmes et leur validation. Le D4.2 contiendra tous les éléments d'implémentation associés.

- **Présentation Tâche 4** : Wissam

- Livrable D4.2 et D4.2 : discussion sur les scénarios pour chaque attaque (en lien avec discussion tâche 3)

Il est prévu d'avoir les résultats des tests unitaires relatifs aux composants de sécurité dans le D3.2 et ceux spécifiques au démonstrateur (par ex gateway) dans D4.3.
Dans D4.2, nous aurons les évaluations relatives à la sécurité et dans D4.3, nous retrouverons les résultats de tests de bout-en-bout réalisés sur le testbed avec le démonstrateur.
Les livrables D4.2 et D4.3 décrieront aussi les environnements, les scénarios, la configuration et seront liés au code fournis.
Dans D4.3 seront listés les protocoles de tests avec liste des tests et scénarios en environnement libre (si possible de faire) et en environnement contrôlé. Ceci sera à rédiger pour fin janvier.

Orange propose d'utiliser un outil de mesure qu'ils ont développé permettant d'évaluer la gateway d'un point de vue utilisateurs (QoE, ressources, connexions sécurisées ou pas, etc.)
PA Bertrand : Voir avec Antoine et Xavier pour coordonner cette campagne de tests

Il serait intéressant de mesurer des métriques réseau de type NFV (scale up / down) en fonction du nombre de requêtes et charges.

- Ouverture Testbed au public

Il est envisagé 2 types de tests :

1) des tests en environnement contrôlé, avec un ensemble d'utilisateurs (par ex étudiants) déroulant les scénarios de tests définis par le projet Doctor. Ceci permet de mesurer exactement ce que nous voulons dans les conditions que nous voulons.
2) des tests sur longue durée avec des utilisateurs volontaires utilisant le testbed pour leurs propres besoins. Cette option permettrait un retour d'expérience sur une longue durée et des jeu de données (éventuellement rejouable). Cependant, il faut que l'UTT et le Loria se renseigne avec leurs universités sur la possibilité technique et juridique de réaliser ce type de tests.

   Il est prévu d'ouvrir le testbed début février (annonce et recherche de candidats maintenant et décision fin janvier). Des tests en environnement contrôlé avec étudiants en groupe pourraient être réalisés en février-mars.
   Selon la correspondante CNIL à l'UTT, il n'y a pas besoin de faire de déclaration CNIL car pas accès aux données personnelles.
   PA Loria et UTT : Voir avec services sur ouverture testbed

   Il faut pouvoir anonymiser les traces dès la capture de données, et pour des raisons de privacy, stocker uniquement les en-têtes, pas la payload (avec outil MMT)
   PA Montimage : S'assurer que les infos stockées par l'outil respectent la vie privée

   Nous avons échangé sur les topologies virtuelles à mettre en œuvre pour le testbed. Pour l'instant, L'UTT utilise la topologie Clara. A voir si une autre serait pertinente et voir si on pourrait rejouer des tests avec une autre topologie (en fonction des traces collectées).

   Il a été discuté de communiquer avec le groupe NDN et voir comment intégrer Doctor au testbed NDN et proposer les outils développés par le projet. A voir plus tard