Audit of Software Defined Networking (SDN) Controllers

Institut Mines-Télécom

Auteurs

Mensah Pernelle
Perdriat Antoine

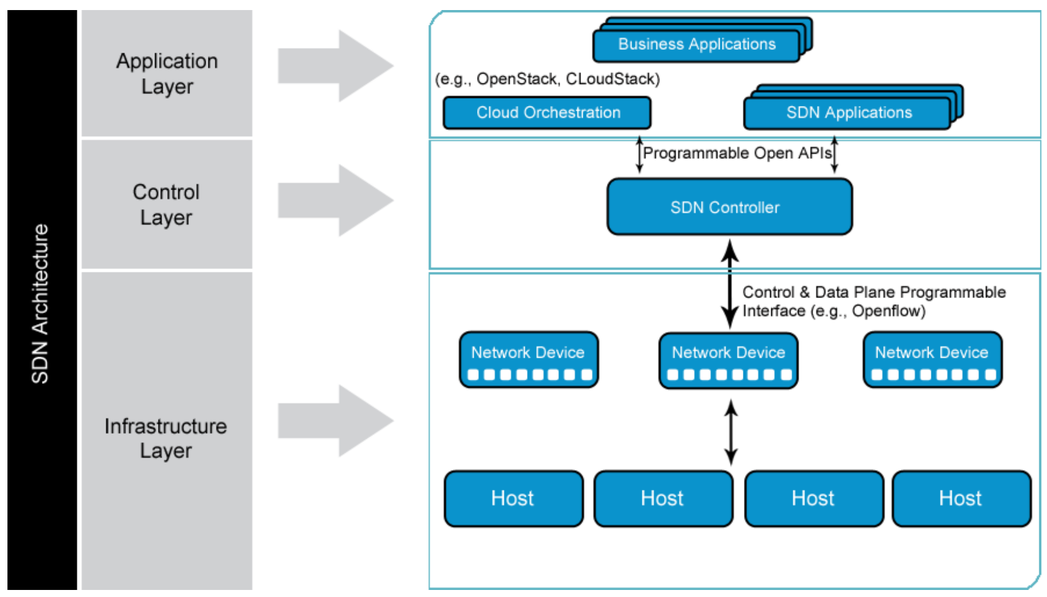
Tuteurs

Grégory Blanc
Joaquin Garcia-Alfaro

L'architecture réseau actuelle : un challenge pour la supervision et l'évolution technologique

Un besoin de programmabilité

- Les réseaux modernes sont constitués de multiples équipements chacun ayant une fonctionnalité particulière et étant potentiellement fourni par un équipementier différent
- Assurer la sécurité et la gestion de ces équipements, du fait de leur diversité et de leur complexité s'avère être de plus en plus difficile.
- D'où la nécessité du SDN, introduisant plus de flexibilité dans le réseau en s'inspirant d'une architecture en couches, rappelant celle des ordinateurs :
  - Couche de contrôle
  - Couche infrastructure
  - Couche applicative



Le contrôleur SDN : une intelligence centralisée, un point de défaillance unique

Un composant à sécuriser

Etant le centre nerveux de la technologie SDN, les contrôleurs sont une cible propice aux attaquants. En effet, l'étude de POX (contrôleur en Python) et Floodlight (contrôleur en Java) met en lumière plusieurs vecteurs de menace :

- Des paquets malicieux forgés par des équipements défectueux ou des attaquants avec pour objectif de créer un déni de service du contrôleur
- Des attaques sur le canal de contrôle entre le contrôleur et le switch pouvant occasionner un déni de service, ou une atteinte à la confidentialité ou à l'intégrité des données
- Des bugs au niveau du contrôleur menant à la compromission de l'ensemble du réseau
- Des attaques ou des vulnérabilités touchant les hôtes du réseau et dont le contrôle permet d'entraver le bon fonctionnement du contrôleur
- Le manque d'un mécanisme d'authentification entre le contrôleur et les applications
- Le manque d'un mécanisme de contrôle d'accès et de sandboxing des applications
- La possibilité d'une fuite d'information concernant entre autres l'architecture du réseau

Scénarios d'attaques mis en oeuvre

Analyse de la robustesse des contrôleurs POX et Floodlight

Les preuves de concept réalisées ont permis d'affecter les critères de sécurités suivants :

- Confidentialité:
  - Réalisation d'attaques Man in The Middle permettant d'observer le canal de contrôle entre le switch et le contrôleur, dû à l'absence de chiffrement
- Disponibilité
  - Réalisation d'applications modifiant le comportement du contrôleur
  - Exploitation du protocole Openflow pour créer un dépassement mémoire au niveau du contrôleur par l'implémentation d'un switch malicieux
  - Exploitation des hôtes entraînant une congestion du canal de contrôle
- Intégrité :
  - Réalisation d'applications malicieuses permettant de modifier les tables de flux du switch

Bien qu'étant une technologie pleine de promesses, le SDN doit encore imposer une implémentation des mécanismes de sécurité au niveau du contrôleur afin de pouvoir proposer une alternative suffisamment fiable pour une exploitation en milieu professionnel.

Projet de fin d'étude VAP SSR

Janvier 2015

Contact pernelle.mensah@telecom-sudparis.eu
antoine.perdriat@telecom-sudparis.eu

Site web