Émulation de réseaux véhiculaires pour la détection d'anomalie

Quentin Ricard
quentin.ricard@laas.fr

15 Mai 2019

LAAS-CNRS
/ Laboratoire d'analyse et d'architecture des systèmes du CNRS

Laboratoire conventionné
avec l'Université Fédérale
de Toulouse Midi-Pyrénées

Sommaire

Contexte

Projet e-horizon : Continental

- Amélioration de l'expérience routière autour de **3** axes :
  1. Sûreté :
     - Ex : Conditions météorologiques, vitesse maximale conseillée ;
  2. Gestion de flotte :
     - Ex : Usure équipement, monitoring consommation ;
  3. Expérience utilisateur :
     - Ex : Prévisions de temps de route, points d'intérêts ;

Implications

- Apparition d'un canal de communication entre les véhicules et le reste du monde.

Problématique

Vecteur d'attaque supplémentaire

- Comment se prémunir contre les nouvelles menaces sur ces nouveaux équipements ?
  - Jeep Cherokee, 2015, (Charlie Miller et Chris Valasek).
  - Nissan Leaf, 2016, (Troy Hunt)
  - Volkswagen/Audi, 2018, (Daan Keuper et Thijs Alkemade)

Détection d'anomalies

- L'application des méthodes existantes de détection d'anomalies au monde automobile.
  - Adapter les algorithmes aux caractéristiques du trafic cellulaire.
  - Adapter les datasets aux voitures connectées.
- Dataset inexistant

Problématique

Vecteur d'attaque supplémentaire

- Comment se prémunir contre les nouvelles menaces sur ces nouveaux équipements ?
  - Jeep Cherokee, 2015, (Charlie Miller et Chris Valasek).
  - Nissan Leaf, 2016, (Troy Hunt)
  - Volkswagen/Audi, 2018, (Daan Keuper et Thijs Alkemade)

Détection d'anomalies

- L'application des méthodes existantes de détection d'anomalies au monde automobile.
  - Adapter les algorithmes aux caractéristiques du trafic cellulaire.
  - Adapter les datasets aux voitures connectées.
- Dataset inexistant

Autobot

Docker

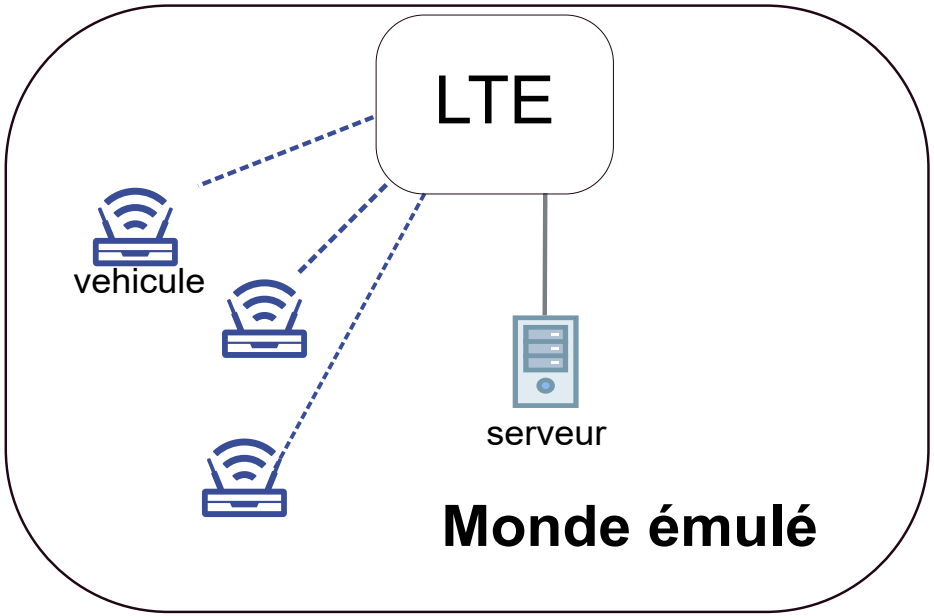
- Émule les nœuds réseau
- Trafic des applications véhiculaires

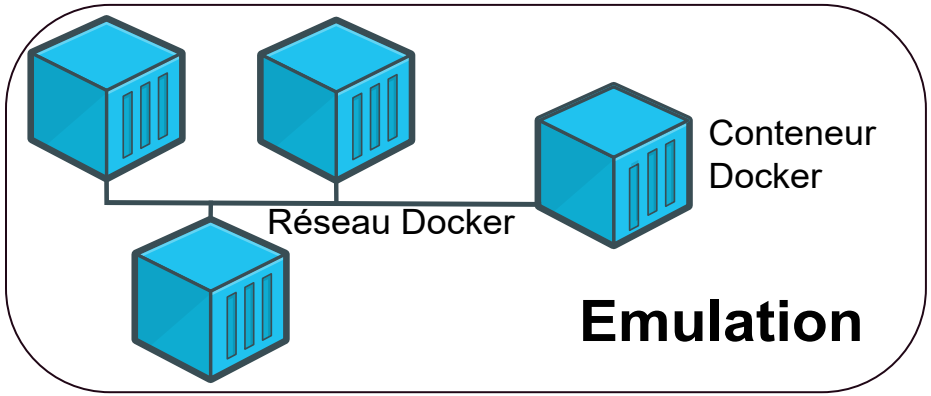
Docker Networks

- Routage
- Gestions Sous-réseaux

Traffic Control

- Manipulation du trafic
- Latence/Perte/Débit





Objectifs

Réplication d'attaques et d'anomalies

- Recherche de réalisme Shiravi *et al.* [2012]
- Attaques de l'état de l'art
- Données télémétriques véhiculaires (ex : Sensoris, NDS)

Analyse

- Capture au niveau IP et génération du dataset
- Détection des anomalies

Conclusion et Ouverture

Autobot

- Peu coûteux
- Rapide à mettre en place
- Suffisamment représentatif pour nos besoins
- Ajout de nouvelles fonctionnalités : infotainment, mises à jours automatiques.

Détection d'anomalies et modèle ontologique

- Représentation des communications du véhicule.
- Pré-classification (véhicule/utilisateur).
- Représentation des anomalies.

Merci

References I

Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali A Ghorbani. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *computers & security*, 31(3) :357–374, 2012.