Reconfiguration d'Architectures pour l'Amélioration de la Résilience des Véhicules Connectés

Soutenance de mi-parcours

Encadrants de Thèse :
Etienne Borde
Ulrich Kühne

Maxime AYRAULT

6 Novembre 2020

Sommaire

Présentation du sujet

État de l'art

- Techniques de défenses dynamiques
- Résilience
- Théorie des jeux

Travaux réalisés

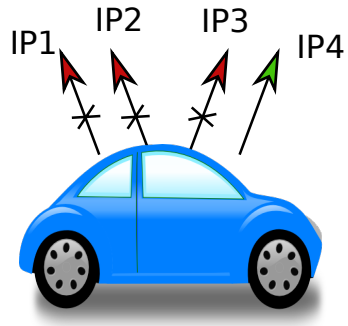
- Définition de l'architecture d'un véhicule
- Défense MTD basée sur la reconfiguration du réseau
- Stratégies de défenses optimales

Travaux futurs

- Amélioration du modèle et prise en compte de la résilience
- Calcul de l'indice de résilience du véhicule

Présentation du sujet - Le contexte

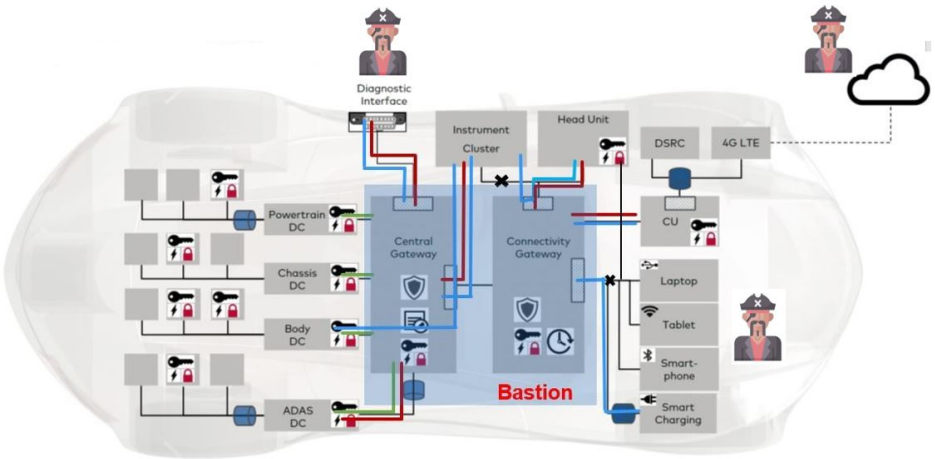
- IoT de plus en plus présent dans la vie courante.
  $\rightarrow$ fortement développé dans l'industrie automobile.



- Cohabitation entre applications critiques (impliquant vies humaines) et applications non critiques (expérience de l'utilisateur).
- Nouvelles attaques non connues au moment de la conception du système qui apparaitront pendant la durée de vie du véhicule
- Objectif : Être capable de s'adapter à toutes formes d'attaques connues ou non.
  $\rightarrow$ Être le plus résilient possible.
  $\rightarrow \Uparrow$ Disponibilité ; = Confidentialité et Intégrité

Présentation du sujet - Trois Types d'Attaquants

- **Attaque physique** : Via diagnostique de la voiture. Objectif : Rajouter des fonctionnalités sur le véhicules pour lesquelles on a pas payé.
- **Attaque courte portée** : Via smartphone/laptop.. Objectif : Prendre le contrôle d'un véhicule proche, ou envoyer de fausses informations au véhicules alentours.
- **Attaque longue portée** : Via WiFi/4G. Objectif : Prendre le contrôle d'une flotte de véhicule.



Etat de l'Art - Techniques de Défenses Dynamiques

- Véhicules limités en puissance calcul et en ressources.
  $\rightarrow$ Utilisation de méthodes de défense légère.
- Deux types de défenses dynamiques complémentaires applicables sur les véhicules : *Moving Target Defense* (MTD) et *Modes Dégradés*.
- Côté proactif : **MTD** [1] : ralentir l'acquisition de connaissances sur le système par un attaquant.
- Côté réactif : **Modes Dégradés** : bloquer la progression d'un attaquant après les défenses percées.
  Aide au retour du système dans état nominal.

1. Gui-linCaiet al. "Moving target defense : state of the art and characteristics". en. In :Frontiers of Information Technology and Electronic Engineering17.11 (nov. 2016)

Etat de l'Art - Moving Target Defense

- Rendre dynamique différents aspects d'un système
  $\rightarrow$ Casser la relation asymétrique attaquant / défenseur.
- Ralentir un attaquant dans l'acquisition de connaissances, la découverte de vulnérabilités et l'exploitation de failles

Les MTD se divisent en 5 catégories [2] :

- Changer dynamiquement la représentation des données
- Utilisation dynamique d'applications
- Modification de l'environnement d'exécution
- Rendre dynamique la plateforme d'exécution
- Configuration dynamique du réseau

2. H.Okhraviet al.Survey of Cyber Moving Target Techniques :en. Rapp. tech. Fort Belvoir, VA :Defense Technical Information Center, sept. 2013.

Etat de l'Art - Efficacité des MTD Lors d'une Attaque

Une attaque est divisée en 5 phases [3] :

1. Reconnaissance
2. Accès
3. Déploiement
4. Lancement
5. Persistence

MTD/ Attack	Reconnaissance	Accès	Déploiement	Lancement	Persistence
Réseau	✓			✓	
Plateforme		✓	✓		✓
Enviromenent d'Execution			✓	✓	
Logiciel			✓	✓	
Donées			✓	✓	

3. H.Okhraviet al. "Finding Focus in the Blur of Moving-Target Techniques". In :IEEE SecurityPrivacy12.2 (mar. 2014)

Etat de l'Art - Résilience

Définition de la Résilience [4]

- The persistence of service delivery that can justifiably be trusted, when facing changes.

Notre Définition de la Résilience

- Se défendre de manière proactive le plus longtemps possible contre toutes formes d'attaques. Une fois ces défenses tombées, revenir rapidement dans un état de fonctionnement nominal grâce à des mécanismes de défenses réactifs.

- Exemple de méthodes visant à améliorer la résilience : *Redondance, Obsfucation, Cryptographie, Monitorat, Isolation*.

4. Laprie, Jean-Claude. "From Dependability to Resilience." International Conference on Dependable Systems and Networks (DSN 2008, 2008, 2.)

Etat de l'Art - Théorie des Jeux

- Problème décisionnel à résoudre ?
  $\rightarrow$ Modélisation du problème grâce à la théorie des jeux [5]
  $\rightarrow$ Analyse sur le modèle afin trouver une/des solution(s)

Exemple : Recherche stratégies défenses optimales en cas d'attaque.

$\rightarrow$ Représentation interractions attaquant / defenseur avec modèle mathématique.

$\rightarrow$ Permet l'observation de l'impact de la configuration système et méthodes défenses sur interactions attaquant / défenseur.

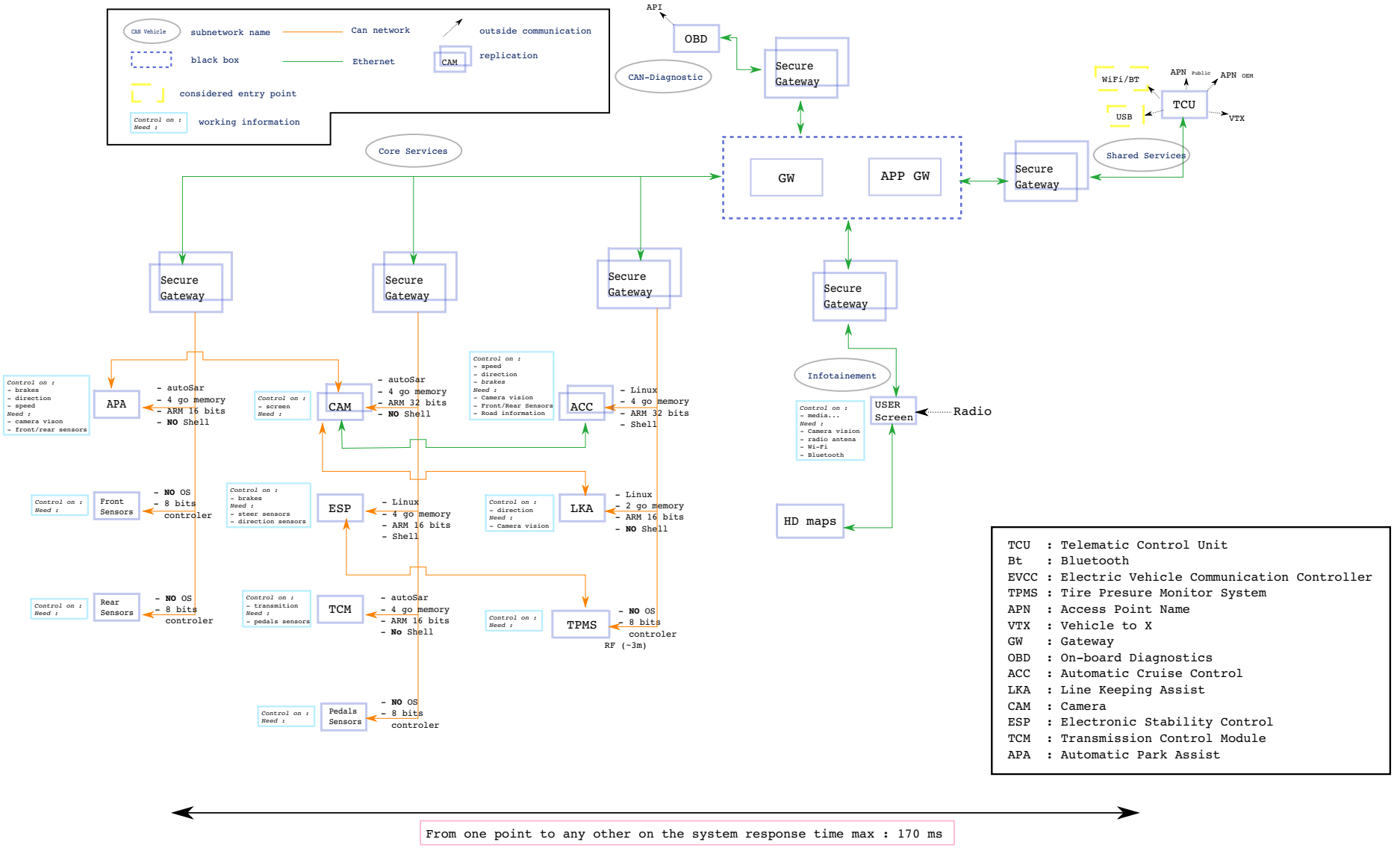
5. Lin Chenet J.Leneutre. "A Game Theoretical Framework on Intrusion Detection in Heteroge-neous Networks". en. In :IEEE Transactions on Information Forensics and Security4.2 (juin 2009)

Etat de l'Art - Analyse sur les Jeux

- La recherche des meilleures stratégies passe par l'analyse de plusieurs 'equilibres [6].
- **Equilibre de Nash** ; joueurs jouent simultanément. D'etermination stratégies dont les deux joueurs ne devraient pas dévier seul.
- **Equilibre de Stackelberg** ; joueurs jouent chacun leur tour. Determination des meilleures stratégies permettant de limiter les gains du second joueur.
- **Minmax**. Permet de minimiser le reward maximum que l'autre joueur pourrait obtenir.

6. Ziad Ismail et al. "A Game Theoretical Model forOptimal Distribution of Network Security Resources".en. In : (2017)

Travaux Réalisés - Architecture Véhicule

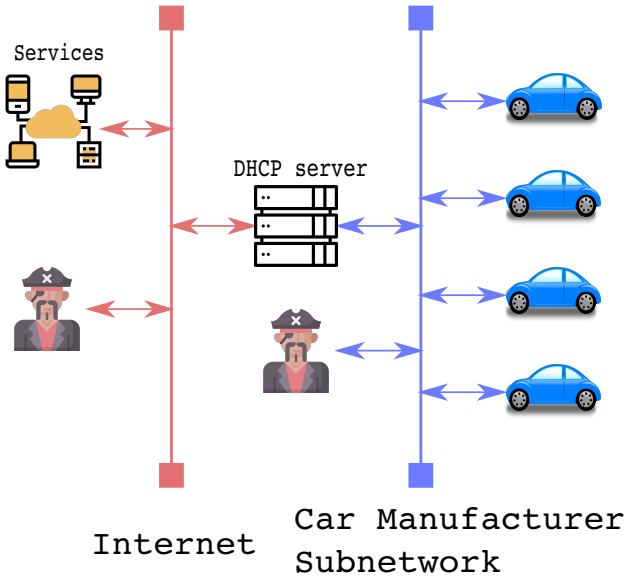


TCU : Telematic Control Unit
Bt : Bluetooth
EVCC : Electric Vehicle Communication Controller
TPMS : Tire Presure Monitor System
APN : Access Point Name
VTX : Vehicle to X
GW : Gateway
OBD : On-board Diagnostics
ACC : Automatic Cruise Control
LKA : Line Keeping Assist
CAM : Camera
ESP : Electronic Stability Control
TCM : Transmission Control Module
APA : Automatic Park Assist

From one point to any other on the system response time max : 170 ms

Travaux Réalisés - Défense MTD Basée sur la Reconfiguration du Réseau

- Méthode permettant cacher un véhicule dans un réseau.
  $\rightarrow$ Changement régulier adresse IP + Limitation impact sur QoS.
- Publication article Workshop MTD associé ACM CCS de 2019 [7].



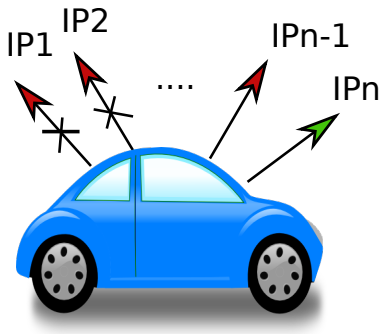
Actuellement :

- Un véhicule = Une adresse IPv4 (appartenant à la plage d'adresse du constructeur)
- Découverte de l'adresse $\rightarrow$ Collecte d'informations du système par attaquant possible.

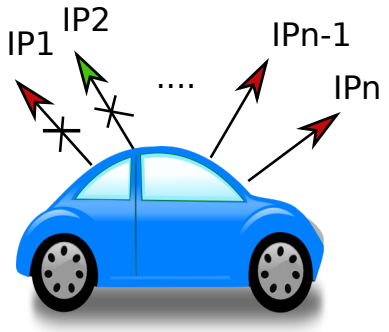
7. Maxime Ayrault, Etienne Borde, Ulrich Kühne. "Run or Hide ? Both ! A Method Based onIPv6 Address Switching to Escape While Being Hidden". In :Proceedings of the 6th ACMWorkshop on Moving Target Defense - MTD'19.

Travaux Réalisés - Principe de notre Méthode

- Un véhicule = *N* interfaces réseaux.
  $\rightarrow$ Plusieurs adresses IP par véhicule.
- Une seule adresse IP active à la fois.
  (Active = Acceptant les messages entrant)
- Rotation périodique de l'adresse IP active.
- Renouvellement adresse IP après utilisation.
- Utilisation *MultiPath TCP* (MPTCP)
  $\rightarrow$ Garantir une qualité de service suffisante.



Rotation périodique

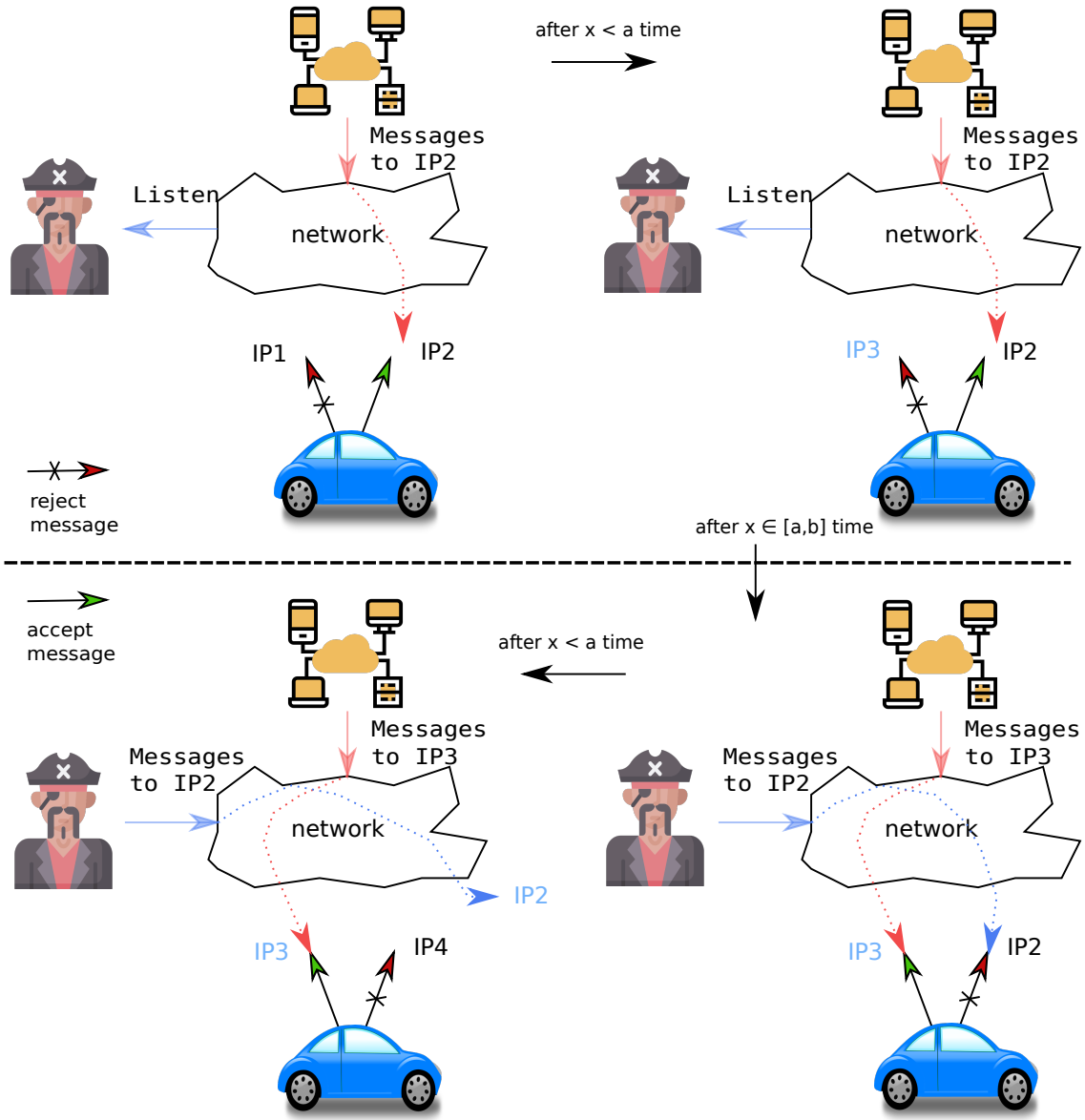


Travaux Réalisés - Différentes versions Méthode

- Version 1 : $N > 2$; Pas de renouvellement adresse après utilisation.
- Version 2 : $N > 2$; Renouvellement adresse après utilisation.
- Version 3 : $N = 2$; Renouvellement adresse après utilisation.

	Version 1	Version 2	Version 3
Coût interface	+++	+++	+
Coût bande passante	+	++	+++
Risque d'attaque DoS	+++	+	+

Travaux Réalisés - Exemple d'Utilisation de la Version 3



Travaux Réalisés - Définition du Jeu

- 2 joueurs : Un attaquant (le hacker) - un défenseur (le système). Nombre fini de mouvements définis.
- Une combinaison mouvement = une fonction reward par joueur. *R_d : Reward Défenseur ; R_a : Reward Attaquant*
- Choix des actions à réaliser
  $\rightarrow$ Dépense d'un budget attribué à chaque joueur.
  P : Budget Défenseur ; Q : Budget Attaquant
- Trouver les meilleures stratégies
  $\rightarrow$ Objectif des deux joueurs = maximiser les rewards obtenus.

Travaux Réalisés - Forme Normale Jeu

- Utilisation des budgets dans les actions :
  q_i : *Se reconfigurer* ; q_i^{not} : *ne rien faire* ; q_i^{deg} : *Passer en mode dégradé* ;
  p_i : *attaquer* ; p_i^{not} : *ne pas attaquer*

- Tableau représentant forme normale du jeu :

	Reconf (q_i)	Rien (q_i^{not})	Degradé (q_i^{deg})
Attaque (p_i)	$R_1^a ; R_1^d$	$R_2^a ; R_2^d$	$R_3^a ; R_3^d$
Pas Attaque (p_i^{not})	$R_4^a ; R_4^d$	$R_5^a ; R_5^d$	$R_6^a ; R_6^d$

- Analyses de différents équilibres $\rightarrow$ determiner les meilleures stratégies.

Futurs travaux

- Adapter le modèle au cas d'étude du véhicule.
- Prise en compte de la résilience dans le modèle du jeu.
- Calcul de l'indice de la résilience.
- Créer un modèle générique du jeu.