Ceci est ma thèse

Vie amoureuse des tétards à Ph7

Maxime Ayrault

A thesis presented for the degree of
Doctor of Philosophy

Department Name
Telecom Paris
France
30 février 2056

Ceci est ma thèse

Vie amoureuse des têtards à Ph7

Maxime Ayrault

Résumé

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Abstract

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Dédicace

À ma Maman adorée...

Remerciements

Je remercie Jean-Do pour ces conseils avisés.....

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

- **CAN** : Controller Area Network.
- **ECU** : Electronic Controller Unit.

Chapitre 1

Introduction

Il est très important, pour celui qui souhaite découvrir, de ne pas limiter son esprit à un seul chapitre de la science mais plutôt de rester en contact avec plusieurs autres.

Jacques Hadamard.

Nous vivons dans l'ère des télécommunications. Les communications constituent, sans aucun doute, l'une des plus importantes révolutions de la science et la technologie.

Ce mémoire de thèse .....

Ce mémoire est divisé en six chapitres et 2 annexes..

Le chapitre 2 contient un rappel sur la théorie....

Le chapitre 3 développe....

Au chapitre 4, expose une application des résultats ....

Le chapitre 5 déjà la conclusion et les perspectives .....

Dans l'espoir de pouvoir intéresser le lecteur curieux, ...

Chapitre 2

La sécurité dans le monde de l'automobile

Ce travail fût présenté en partie à la conférence des sourds-muets unijambistes à Quibéron en avril 1994.

Maxime Ayrault

2.1 La révolution logicielle

Le logiciel embarqué est une des innovations clé dans le monde automobile. D'après l'article de Robert Charette (Charette 2009) paru dans IEEE Spectrum, la première voiture embarquant un logiciel était la Oldsmobile Toronado de General Motors en 1977. La Toronado avait une unité de contrôle électronique (ECU) qui gérait la synchronisation de l'allumage des bougies (spark timing). En 1978, General Motors proposait, en option sur ses Cadillacs, un ordinateur de bord qui pouvait afficher la vitesse, le niveau du réservoir d'essence, les informations sur l'état du véhicule. Ce logiciel s'exécutait sur une version modifiée du processeur Motorola 6802 et faisait 50.000 lignes de code. Depuis, de plus en plus de fonctions ont été réalisées par du logiciel. Afin de limiter le nombre de câbles dans une voiture, les capteurs ont été décentralisés et connectés à un réseau interne (réseau CAN). Le logiciel a également permis de créer de nouvelles fonctions pour les voitures.
Une voiture actuelle est maintenant devenue une plate-forme logiciel sur roues. Une voiture grand public contient entre 30 et 50 unités de contrôle électronique effectuant la gestion de multiples systèmes (voir 2.1).

Air bag	ABS	Système d'alarme
La climatisation	Le régulateur de vitesse	Le régime moteur
Les clignotants	Les feux	Le klaxon
La gestion des sièges	Le système de navigation	Le système audio
La pression des pneus	La gestion des portes et vitres	...

TABLE 2.1 – Système logiciel dans une voiture

En 2009, Alfred Katzenbach, le directeur des Technologies Informatique Chez Daimler, a annonçé que le système navigation et audio sur une Mercedes-Benz S-class contient plus 20 millions de lignes de code et que la voiture contienait pratiquement autant d'unité électronique qu'un Airbus A380 (si on exclut le système de divertissement en vol) (**Cha09**). Les logiciels dans une voiture grossissent à une vitesse exponentielle en taille et en complexité. En 2010, certaines voitures avaient 10 millions de lignes de code. En dix ans, le volume du logiciel a augmenté par un facteur 15, pour environ 150 millions de lignes. Aujourd'hui, le Model S de Tesla est équipée d'un écran tactile de 17 pouces basé sur un système d'exploitation Linux qui contrôle quasiment toute les fonctions utilisateurs de la voiture. En fait, il n'y a plus que 2 boutons manuel non gérés par du logiciel sur un Model S ; le bouton pour les feux de détresse et le bouton de la boîte à gants.

Un effet secondaire est sur la complexité des fonctions proposées aux conducteurs. Il n'est pas rare que les manuels utilisateurs des voitures fassent maintenant plus de 500 pages pour expliquer l'ensemble des fonctions logiciel. D'un autre côté, on estime qu'un conducteur moyen n'utilise pas plus de 20% des fonctions implémentées par du logiciel. Les constructeurs automobiles commencent à se poser la question sur une limitation des fonctions réalisées par du logiciel. Par exemple, est-il vraiment nécessaire que la lumière du plafonnier d'une voiture s'éteigne de façon progressive ?

L'augmentation du logiciel a également d'importantes conséquences sur la façon d'entretenir et de réparer une voiture. On estime que plus de 50% des unités électroniques remplacées n'ont pas d'erreur (logiciel ou matériel). Le garagiste remplace fréquemment une pièce car il ne sait pas quelle est la cause principales de la panne. La principale activité des garagiste consiste à téécharger les nouvelles versions du logiciel. Sur les voitures Tesla, les mises à jour logiciel, qui incluent les corrections du logiciel et les nouvelles fonctionnalités sont téléchargées dans la voiture via le réseau cellulaire sans intervention d'un garagiste.

Aujourd'hui, le coût du logiciel et de l'électronique représente entre 35 à 40% du coût d'une voiture.

Todo list 1. Introduire Automotive Open System Architecture (AUTOSAR). Une solution pour réduire le coût du logiciel en augmentant l'interopérabilité entre les constructeurs.

L'introduction du logiciel a permis d'avoir des voitures plus sûrs et moins polluantes mais a également introduit une nouvelle menace ; la *sécurité informatique des voitures*.

2.2 Architecture voiture

Todo list 2. Commencer a présenter les différentes couches logiciel.

the following four stacks could become the basis for upcoming generations of cars in five to ten years :

- *Time-driven stack*. In this domain, the controller is directly connected to a sensor or actuator while the systems have to support hard real-time requirements and low latency times ; resource scheduling is time based. This stack includes systems that reach the highest Automotive Safety Integrity Level classes, such as the classical Automotive Open System Architecture (AUTOSAR) domain.
- *Event- and time-driven stack*. This hybrid stack combines high-performance safety applications, for example, by supporting ADAS and HAD capability. Applications and peripherals are separated by the operating system, while applications are scheduled on a time base. Inside an application, scheduling of resources can be based on time or priority. The operating environment ensures that safety-critical applications run on isolated containers with clear separation from other applications within the car. A current example is adaptive AUTOSAR.
- *Event-driven stack*.This stack centers on the infotainment system, which is not safety critical. The applications are clearly separated from the peripherals, and resources are scheduled using best-effort or event-based scheduling. The stack contains visible and highly used functions that allow the user to interact with the vehicle, such as Android, Automotive Grade Linux, GENIVI, and QNX.
- *Cloud-based (off-board) stack*. The final stack covers and coordinates access to car data and functions from outside the car. The stack is responsible for communication, as well as safety and security checks of applications (authentication), and it establishes a defined car interface, including remote diagnostics.

`https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture`

`https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/pure-play-so html`

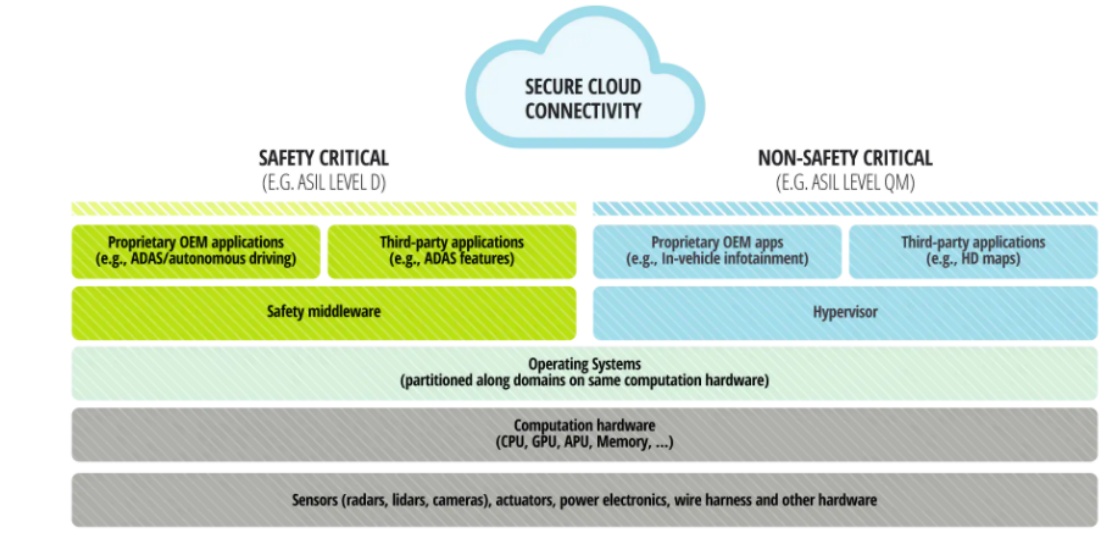

FIGURE 2.1 – Architecture générique

Bla bla bla

2.3 Principes de la sécurité informatique

La sécurité informatique est construite sur 3 piliers (CIA triad).

— La *confidentialité*. L'objectif consiste á éviter la divulgation d'informations sensibles et/ou de protéger les accès non authorisés ressources sensibles. Autrement dit, la confidentialité implique la protection des données (resp. ressources), en donnant accès à ceux qui sont autorisés à les lire (resp. à les utiliser) tout en interdisant aux autres d'apprendre quoi que ce soit sur son contenu (ou son existence).

— L'*intégrité*. L'objectif est de protéger ou de minimiser les modifications non authorisées de données et/ou ressources sensibles. Autrement dit, l'intégrité implique de préserver le contenu des données et de détecter si une donnée ou une ressource a été altérée depuis sa derniére écriture par une personne authorisée.

— La *disponibilité*. L'objectif est de maintenir le système opérationel pour rendre le service aux l'utilisateurs.

FIGURE 2.2 – Les pilers de la sécurité informatique

Les principales techniques utilisées pour garantir ces 3 propriétés sont :

— *Chiffrement (Encryption)* : La transformation de l'informations originale (appelé clair) à l'aide d'une clé de chiffrement, de telle sorte que les informations transformées (appelé chiffré) ne puissent être interprétées que par un autre utilisateur ayant connaissance de la clé de déchiffrement (qui peut, dans certains cas, être identique à la clé de chiffrement). Pour être en sécurité, un algorithme de chiffrement doit rendre extrêmement difficile pour quelqu'un de déterminer tout ou partie des informations clairs sans connaissance de la clé de déchiffrement ou faiblesse de l'algorithme de chiffrement.

— *Authentification (Authentication)* : La détermination de l'identité qu'un sujet (personne, logiciel ou équipement). Cette détermination peut être effectuée par plusieurs moyens. Il est généralement basé sur une combinaison de quelque chose que la personne connaît (Something you know) comme un mot de passe ou un code PIN, quelque chose le sujet possède (Something you have) comme une carte à puce contenant des clés secrètes un téléphone pour recevoir un code, un passeport, ou quelque chose la personne est (Something you are) comme une empreinte digitale.

— *Contrôles d'accès (Access Control)* : Ensemble de règles et politiques de sécurité qui limitent l'accès aux informations aux sujets (personnes et/ou systèmes) ayant un *besoin d'en connaitre*. Ce besoin d'en connaitre est déterminé suite à l'authentification correcte du sujet, de par son identité ou rôle. Un ensemble de règles est pré-définie par le gestionnaire de la sécurité informatique en se basant sur la politique de sécurité.

— *Signature (Signature)* : La signature d'une information a deux objectifs ; assurer que l'information signée n'a pas été altérée depuis la signature et authentifier la source de l'information (non-repudiation). La signature consiste en un chiffre dépendant d'une clé secrète connue uniquement par le sujet signant l'information et du contenu du message à signer. Une signature est vérifiable, sans connaitre la clé secrète, par une partie tierce en cas de litige entre parties. Si le contenu du message ou la signature est modifié, la correspondance entre le contenu initial et message et sa signature sera invalide permettant de détecter l'altération et de rejecter l'information. De façon, symétrique, si

le contenu du message et sa signature correspondent alors la source de l'information ne pourra pas nier avoir signé l'information car elle est la seule à connaitre la clé secrète.

— *Responsabilité (Accountability)* : La capacité de rendre le sujet responsable de ces actions. Ceci est réalisé en s'appuyant sur des journaux d'audit (audit log). Une fois le sujet correctement authentifié, toutes ces actions sont enregistrées sous forme d'événements dans un journal d'audit. En cas d'investigation ou de façon périodique, le gestionnaire de la sécurité informatique peut réaliser un audit des journaux pour identifier la source potentielle d'une attaque.

— *Sensibilisation à la sécurité (Security awareness)* : La principale source de risque pour une organisation ne provient pas de faiblesse dans la technologie des équipements mais d'actions (ou d'inaction) de la part des utilisateurs du système. Afin de limiter ce risque, il est nécessaire de former les utilisateur aux diiférents risques informatiques et aux bonnes pratiques pour assurer le niveau de sécurité requis.

— *Sécurité physique (physical security)* : Mise en place de barrières physiques pour limiter l'accès aux ressources sensibles. Ces barriÃ¨res comprennent sont mutiples comme le gardiennage, la vidéo-surveillance, les serrures sur les armoires et les portes, les chambres fortes, l'utilisation de matÃ©riaux insonorisants, ou même la construction d'équipement renforcé (tempest) afin que les signaux électromagnétiques ne puissent pas entrer ou sortir.

— *Tolérance aux fautes (fault tolerance)* : Ensemble de techniques peuvent être utilisées pour garantir le systéme en opération.

	Confidentialité	Integrité	Disponibilité
Chiffrement	✓		
Authentification	✓	✓	
Contrôles d'accès	✓	✓	
Signature		✓	
Responsabilité	✓	✓	
Sensibilisation à la sécurité physique	✓	✓	✓
Sécurité physique	✓	✓	✓
Tolérance aux fautes			✓

Table 2.2 – Principales méthodes de la sécurité informatique

Dans le reste de la thèse, nous concentrerons sur la disponibilité des systèmes embarqués.

2.4 Le risque cybersécurité pour l'automobile

L'ajout de logiciels et de connectivité....
3 niveaux d'attaques :
— *Attaques physiques.*

  - Attaque via la prise diagnostique de la voiture. L'objectif est de pouvoir modifier les caractéristiques de la voiture et/ou de rajouter des options sur la voiture. Les logiciels d'une voiture sont hautement configurables. Un même logiciel est installé sur plusieurs gammes de véhicules d'un constructeur. La différenciation entre les deux modèles s'effectue par le paramtrage du logiciel. Si un attaquant à la possibilité de modifier ces paramètres, il peut activer des fonctions optionnelles de la voiture ou modifier les caractéristiques moteur pour booster le véhicule.
  - Attaque via la prise USB de la voiture. L'objectif est de pouvoir créer un point d'entrée pour une attaque courte ou longue port'ee sur le véhicule. La prise USB peut être connectée sur un équipement radio qui permet d'étendre la portée de l'attaque.

- *Attaque courte portée* L'objectif est de pouvoir prendre le contrôle du véhicule, d'envoyer de fausses informations ou de bloquer les communicatiosn aux véhilcules aux alentours. De plus en plus de voitures ont un système d'ouverture de portes et de démarrage sans clé.Par exemple, votre voiture est garée devant votre maison et les clés sont sur le petit d'entrée. Un attaquqant peut insérer un équipement radio entre la clé et la voiture (attaque par relais). Un côté est proche de la voiture, lautre côté est connecté à une antenne scannant les fréquences radio de la clé. Ceci permet d'ouvrir et/ou de d'emarrer la voiture même quand les clés du véhicule sont hors de portée de la voiture. Une fois que l'antenne a accroché la fréquence de la clé, elle relaye son signal sur l'équipement proche du véhicule. La voiture a ainsi l'impression que le propriétaire est proche et ouvre les portes et autorise la démarrage. Le véhicule peut être volé sans effraction (voir `https://www.youtube.com/watch?v=_cua7BFX-Qk` pour un video d'attaque relais). Un autre exemple, consiste à brouiller le signal pour la fermeture centralisée d'un véhicule. Le conducteur appuie sur le bouton de fermeture centralisée de sa clé, il a le sentiment que sa voiture est correctement fermée. Mais si le signal est brouillé, la voiture est ouverte et un attaquant peut facilement ouvrir un porte pour voler des affaires dans la voiture.

- *Attaque longue portée.* L'objectif est de prendre le contrôle à distance d'un véhicule. Un des fameux exemple de ce type d'attaque est la prise de contrôle d'une Jeep Cherokee par 2 attaquants ; Andy Greenberg conduisait sa voiture sur l'autoroute vers Saint-Louis, roulant 70̀ mph. 2 hackers Charlie Miller et Chris Valasek sont installés dans leur canapé avec leur laptop ouvert. Dans un premier temps, la climatisation de la voiture s'est affol'ee, puis, une image des 2 hackers est apparue sur l'écran de la voiture, la radio a changé de station et le volume a fortement augmenté, Mr Greenberg ne pouvait pas contrôler le volume de la radio ni la station. Ensuite la voiture s'est arrêtée toute seule. (voir Miller et Valasek 2015 pour le détail de l'attaque)

Chapitre 3

La théorie des jeux

Il est très important, pour celui qui souhaite découvrir, de ne pas limiter son esprit á un seul chapitre de la science mais plutôt de rester en contact avec plusieurs autres.

Jacques Hadamard.

3.1 Présentation

La théorie des jeux est la science de la prise de décision stratégique. La théorie des jeux a été utilisée dans des sciences aussi diverses que la biologie évolutionniste, le management des décisions (politique) et l'économie. Elle peut être définie comme l'étude de modèles mathématiques des conflits et coopérations entre décideurs intelligents et rationnels. La théorie des jeux fournit des techniques mathématiques générales pour analyser des situations dans lesquelles deux personnes ou plus prennent des décisions qui s'influencent mutuellement.

Dans le langage de la théorie des jeux, un jeu fait référence à toute situation impliquant deux sujets ou plus. Les sujets impliqués dans un jeu peuvent être appelés les *joueurs*. Comme indiqué dans la définition ci-dessus, il y a deux hypothèses de base que les théoriciens des jeux font généralement à propos des joueurs : ils sont rationnels et intelligents. Chacun de ces adjectifs est utilisé ici dans un sens technique qui nécessite quelques explications. Un décideur est rationnel s'il prend des décisions de manière cohérente de ses propres objectifs. En théorie des jeux, en s'appuyant sur le fondamental résultats de la théorie de la décision, nous supposons que l'objectif de chaque joueur est de maximiser la valeur attendue de son propre gain, qui est mesuré en une certaine échelle d'utilité. L'idée derrière un *décideur rationnel* est que les actions sélectionnées (nommées *stratégies*) maximiseront les bénéfices d'utilité attendus par le joueur. Cette idée remonte au moins à Bernoulli (1738), mais la justification moderne de cette idée tient à Von Neumann et Morgenstern (1947) ([xx]).

Pour expliquer les concepts de la théorie des jeux, prenons un exemple ; "*l'évitement de la congestion du réseau internet*". Le réseau internet est basé sur le protocole

TCP/IP. En TCP/IP, un fichier est découpé en paquets qui transitent entre les différents noeuds du réseau entre l'émetteur et le récepteur. Chaque fois que le récepteur reçoit un paquet, il envoie un accusé de réception à l'émetteur. De cette façon, le lémetteur sait que le paquet est bien arrivé. Le protocole TCP/IP cherche à augmenter le débit du réseau jusqu'à sa saturation. Lorsque l'un des noeuds du réseau est saturé, il efface des paquets jusqu'à désaturer. L'émetteur ne recevant plus d'accusé réception pour un paquet va le ré-émettre après une certaine temporisation (géré par l'algorithme d'évitement de congestion). Si tous les émetteurs suivent cette règle, cela permet de désaturer le noeud pour le bénéfice de l'ensemble des utilisateurs. Cependant, il est possible pour certains émetteurs de violer cette règle et de ré-émettre le message sans latence.

Ce comportement peut être modélisé en théorie des jeux. Imaginons, deux personnes utilisant Internet. Elles ont deux choix possibles :

— Utiliser la version correct de l'algorithme d'évitement de congestion du réseau. Cette stratégie est notée C.
— Utiliser une version défectueuese de l'algorithme d'évitement de congestion du réseau. Cette stratégir est notée D.

Le comportement du réseau est le suivant ; si les 2 personnes choisissent la stratégie C, chaque paquet sera retardé de 2ms. Si les 2 personnes choisissent la stratégie D, chaque paquet sera retardé de 4ms. Si une des personnes choisit l'action C et l'autre l'action D, le premier voit ses paquets retardés de 6ms et le second voit ses paquets reçus sans retard. Bien sûr, chaque personne est rationnel et cherche á augmenter son débit, c'est à dire dans notre exmple, à minimiser le retard de ses paquets.

Definition 1. Un jeu peut être modélisé par un triplet $< N, S, u >$ avec :

— N représente les joueurs. $N = \{1, 2, \ldots, n\}$ est un ensemble de cardinal n (nombre de joueurs dans le jeu).
— S représente l'ensemble des combinaisons de stratégies possibles pour l'ensemble des joueurs $S : S_1 \times S_2 \times \ldots \times S_n$ avec S_i l'ensembles des stratégies possibles pour le joueur i. Tous les joueurs n'ont pas n'ecessairement les même stratégies et certaines combinaisons de stratégies peuvent être impossibles.
— u représente la fonction de $u : S \to \mathbb{R}^n$ qui associe à chaque combinaison de stratégie une valeur d'utilié avec pour chaque u_i :
  — une valeur négative représentant une perte pour le joueur i
  — une valeur positive représentant un gain pour le joueur i

Il est plus commode de représenter la fonction d'utilité pour le joueur i comme $u(S_i, S_{-i})$, avec $S_{-i} = (s_1, s_2, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$.

Pour notre exemple, nous avons :

— 2 joueurs, $N = \{1, 2\}$
— les stratégies possibles pour les 2 joueurs sont identiques $S_1 = S_2 = \{C, D\}$. Et l'ensemble des combinaisons de stratégies possibles est défini comme $S = \{(C, C), (D, C), (C, D), (D, D)\}$
— la fonction utilité peut être représentée par la matrice suivante :

$Joueur_1$ \ $Joueur_2$	C	D
C	(2,2)	(6,0)
D	(0,6)	(4,4)

Bla bla bla

Chapitre 4

Expression de la résilience

Il est très important, pour celui qui souhaite découvrir, de ne pas limiter son esprit à un seul chapitre de la science mais plutôt de rester en contact avec plusieurs autres.

Jacques Hadamard.

4.1 Section Title

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

A	B	C
1	2	3
4	5	6

Table 4.1 – very basic table

Chapitre 5

Conclusions et perspectives

Je vois refléter dans mon miroir tout mon passé et tout mon avenir.

J. Cortázar.

5.1 Les leçons apprises

Aucune !

5.2 Les frontières de la recherche

The sky is the limit...

Bibliographie

Charette, Robert N. (2009). “This car runs on code”. In : *IEEE Specturm* 7649.

Miller, Charlie et Chris Valasek (2015). *Remote exploitation of an unaltered passenger vehicle*. URL : `http://www-cs-faculty.stanford.edu/~uno/abcde.html`.

Annexe A

Ma belle annexe

A.1 Introduction

La théorie....

Ceci est une appendice...