Problématique :

Posséder et fabriquer des véhicules est un passe-temps et une nécessité, qui a été menacé par un enjeux sociatal depuis les temps anciens, ce qui est le vol. Alors, comment agir sur la sécurité des véhicules contre le vol ? Quelle est la méthode qu’on a choisie pour attaquer ce problème ? Et jusqu’à quel point on peut dire que cette méthode est efficace ?

Bibliographie commenté :

Un **véhicule** est « ce qui sert à transmettre, à transporter » 1

Il a été présumé depuis longtemps que nūbalum représentait un nom de char, tandis que J.-M. Durand a proposé de voir dans ce véhicule une sorte de chaise à porteurs ou de palanquin 2

Le vol de véhicules à moteur est un crime qui touche beaucoup de Canadiens, aussi bien directement qu'indirectement. Le Bureau d'assurance du Canada a estimé à plus de 1 milliard de dollars par année le fardeau financier pour les consommateurs, la police, les compagnies d'assurances et les gouvernements. Les véhicules volés qui sont impliqués dans des poursuites policières ou des actes de conduite dangereuse peuvent provoquer des blessures et même des décès chez d'innocentes victimes 3

L’un des composants les plus importants des véhicules, et ceci depuis plusieurs générations de voitures, n’est même pas un élément interne ou fixe dudit véhicule. Il s’agit de la clé de contact, qui assure à la fois sécurité et confort au conducteur, en lui permettant de verrouiller ou de déverrouiller son véhicule directement via cet outil ou à distance.

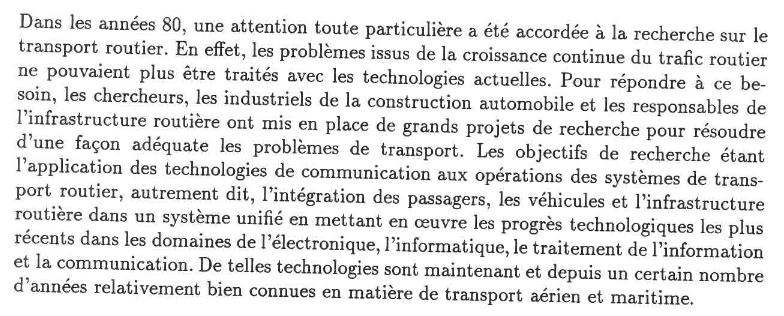
Les clés de contact sont des **éléments de sécurité** essentiels au bon fonctionnement des automobiles. Leurs différentes missions, à savoir permettre le démarrage grâce à l’empreinte spécifique et unique d’une clé et du contact, ou encore verrouiller l’ensemble des portières lorsque l’usager laisse son automobile en stationnement, en font un élément incontournable.

Il existe 3 types de clés différents, dépendant principalement de l’âge de l’automobile à laquelle chaque clé est associée :

* les clés simples
* les clés à transpondeur
* les clés à transpondeur cryptographique

Il s’agit du modèle de clé le plus ancien et le plus simple à reproduire si l’usager a besoin d’un double. En effet, ces modèles de clés ne comprennent aucun élément électronique, et comportent uniquement une **clé métallique**, qui sera ensuite accompagnée d’une coque en plastique. Ce type de clé permet d’**ouvrir les portières et le coffre du véhicule** indépendamment des autres portières. Comme toutes les clés de contact, elle est unique et permet de [démarrer une seule voiture](https://www.ornikar.com/permis/conseils-conduite/demarrer-arreter) 4

Les voleurs s’introduisent dans le domicile de leur victime (généralement sans violence) et dérobent les clés de la voiture posées dans l’entrée avec le portefeuille, le sac à main ou le téléphone portable (phénomène du « Homejacking ») 5

6

L’une des principales priorités des constructeurs automobiles est généralement d'assurer la sécurité de leurs usagers. Cette nécessité de garantir la sécurité des usagers passe notamment par [l’ajout d’équipements](https://www.ornikar.com/code/cours/mecanique-vehicule/technologie-assistance), qu’ils soient en option ou de série, comme le verrouillage centralisé.

Le **verrouillage centralisé** est un équipement, pouvant être proposé en option ou de série dans une voiture, qui permet à un automobiliste qui le souhaiterait de **verrouiller l’ensemble des portes** de son véhicule grâce à une seule et unique action.

Il peut exister différentes commandes pour **activer ou désactiver** le verrouillage centralisé, selon si l’usager se trouve à l’intérieur ou à l’extérieur du véhicule lorsqu’il se décide à l’utiliser.

**L’utilité du verrouillage centralisé**

L’objectif principal du verrouillage centralisé est de permettre aux usagers de se protéger rapidement en cas de risque de vol. Ces risques peuvent arriver alors que les passagers sont dans la voiture, comme lors d’un **carjacking** ou d’un **vol de sac à main**, mais également alors que les usagers sont loin de leurs véhicules.

En effet, grâce au verrouillage centralisé, les automobilistes peuvent **s’assurer rapidement et facilement** que les portes de leur véhicule sont bien verrouillées, ce qui pourra dissuader, ou au moins potentiellement ralentir, des malfaiteurs souhaitant forcer le véhicule pour le voler, lui ou son contenu.

Mais s’il permet d’empêcher les portières de s’ouvrir depuis l’extérieur, le système de verrouillage centralisé ne permet généralement pas de verrouiller les portières pour qu’elles ne puissent **pas être ouvertes depuis l’intérieur** non plus. Ceci est cependant possible sur certains modèles de véhicules, ou en activant le système de [verrouillage pour enfants](https://www.ornikar.com/code/cours/securite/dispositif-enfant). 7

De plus en plus de véhicules sont équipés d’une **clé de voiture sans contact**. C’est une solution pratique et rapide, plus besoin de sortir sa clé, il suffit de l’avoir en poche pour que le véhicule puisse s’ouvrir et démarrer. Vous revenez du supermarché et vous avez les bras chargés ? Vous êtes pressés par le temps ? La clé de voiture sans contact est votre meilleure amie ! Elle doit être à proximité du véhicule afin de recevoir le signal émis par cette dernière.

Le problème, c’est qu’elle peut vite devenir votre pire ennemie ! En effet, de plus en plus de vols de voitures sont recensés car la **hack de la clé** n’est pas si compliqué. 8

Since the radio signal is transmitted in a proximity open area around the automobile, security is a very critical concern. Car thief can use an inexpensive radio scanner to receive the radio signal between the automoile and key fob. A tech-savvy car thief can then analyze the intercepted radio pattern and deduce certain security characteristics to crack the remote keyless system. Conventionally, the remote keyless system works on a relatively straightforward way in which the settings of a DIP switch component in a circuitry specify the intended communication source and target. Typically, there is no cryptographic measure taken. The car thief can simply intercept the radio pattern, and then masquerade as the car owner to spoof the car receiver. This kind of the remote keyless system provides a poor security capability to the automobile. 9

Références :

Définitions [lexicographiques](http://www.cnrtl.fr/lexicographie/Véhicule/0) [[archive](http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fwww.cnrtl.fr%2Flexicographie%2FV%25C3%25A9hicule%2F0)] et [étymologiques](http://www.cnrtl.fr/etymologie/Véhicule/0) [[archive](http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fwww.cnrtl.fr%2Fetymologie%2FV%25C3%25A9hicule%2F0)] de « Véhicule » (sens IA) du [*Trésor de la langue française informatisé*](https://fr.wikipedia.org/wiki/Tr%C3%A9sor_de_la_langue_fran%C3%A7aise_informatis%C3%A9), sur le site du [Centre national de ressources textuelles et lexicales](https://fr.wikipedia.org/wiki/Centre_national_de_ressources_textuelles_et_lexicales)

LesvéhiculesterrestresdanslestextesdeMari.I.Lenūbalum\*

Article de Juristat —Vols de véhicules à moteur au Canada, 2007 par Mia Dauvergne

<https://www.ornikar.com/code/cours/mecanique-vehicule/demarreur/cle-contact>

<http://www.sours.fr/event/voisins%20vigilants%202015/Conseils-G.pdf>

<https://tel.archives-ouvertes.fr/tel-00959734/document>

<https://www.ornikar.com/code/cours/mecanique-vehicule/demarreur/verrouillage-centralise>

<https://blog.zenpark.com/les-cles-de-voiture-sans-contact-fausse-bonne-idee/>

AES Security Protocol Implementation for Automobile Remote Keyless System

Objective :

Dans le but de plus sécuriser les véhicules contre le vol dans notre vie quotidienne j’ai visé d’agir sur le signal de la vie par des methodes qui soit :

* Multiplier le nombre des signaux des voitures ;
* Comment bien structurer les voitures pour avoir un système sécurisé .

Paroles :

1 : Bonjour honorable jury aujourd’hui j’ai le plaisir de vous présenter mon TIPE intituler Système antivol des véhicules qui a pour mission de protéger les véhicules contre tout risque de vol assurant ainsi la sécurité ‘automobile’ qui est un axe des Enjeux Sociétaux.

2 : Le déroulement de ma présentation va respecter le plan suivant ;

Tout d’abord, on va commencer par une simple introduction qui va nous permettre de localiser par rapport à mon sujet.

Ensuite, on va passer à quelques notions de bases de la télécommunication qui vont nous servir à mettre l’accent sur les diverses vulnérabilités de la transmission de signal qui peut être intercepter d’une façon ou d’une autre.

En fait, pour assurer la sécurité de notre véhicule, on va traiter deux signaux, le premier est un signal radiofréquence à courte portée générer par la clé assurant la gestion d’accès au véhicule et qui doit être protéger contre toute tentative d’interception, le deuxième est généré par un système informatique permettant de fournir la géolocalisation du véhicule en cas du vol.

Ce qui va nous amener ensuite à formuler notre problématique liée à fournir des solutions technologiques susceptible d’assurer un niveau de sécurité rassurant.

Et finalement, on va conclure sur l’aspect problématique de la notion de la sécurité qui doit surmonter les défis liés à l’évolution de la machine contre l’humain.

4 : Le véhicule est un bien assez inaccessible qui nécessite un investissement relativement lourd par rapport à la capacité d’achat d’individu marocain ; d’où la nécessité de la sécurité contre toute tentative de vol .

5 : En effet, D’après un article de l’hebdomadaire marocain l’observateur du Maroc & d’Afrique ; 2000 cas de vol sont déclarés annuellement au Maroc .

6 : Maintenant on va passer à la partie de conce….. qui va nous servir à expliquer la gestion d’accès au véhicule via le signal générer par la clé est transmis au calculateur du véhicule grace à la télécommunication.

7 : …

8 : Pour réussir toute tentative de communication on a besoin de plusieurs facteurs.

Tout d’abord un émetteur qui va envoyer un message sur un support de communication en respectant un Protocol de communication compris par l’émetteur et le récepteur, cette communication peut etre classer suivant le sens de flux de communication

En effet, si seul l’émetteur qui diffuse le message comme le cas des émission radios, en parle d’une communication simplex, par contre si les deux peuvent envoyer le message mais pas simultanément on parle d’une communication Half-duplex comme le cas des Talki Walki et finalement on trouve le full-duplex qui offre la possibilité de communiquer à la fois.

9 : On peut également classer les modes de transmission en se basant sur le support physique de transmission, soit filaire ou sans fil, pour la communication filaire le fil peut transmettre un signal électrique (bruits et faible porté) ou un signal lumineux voyageant à la vitesse de la lumière, et pour la communication sans fil, on trouve deux familles une portant une Onde Electromagnétique par exemple …… et l’autre Signal Sonore par exemple …. //// ………. ATTENTION Recherche

10 : Pour unifier le Protocol de la communication utilisée par divers équipementiers qui opère dans les divers pays de la culture diffèrent le modèle OSI est étable .

Pour vous expliquer le principe derrière ce modèle qui a 7 couches prenant l’exemple d’un utilisateur en interaction avec une application de chat installée dans son terminal.

Nous allons décrire les couches de haut en bas car la couches supérieure est la couche Application ou la couche 7 ; c’est la couche avec laquelle la plupart des utilisateurs interagissent et reconnaitrons

La couche Application fournit des services réseau à l »utilisateur final qui fonctionnent avec les données que le client utilise. L’un de ces protocoles peut etre http qui est utilisé avec les navigateurs Web tels que Google Chrome, Firefox et Internet Explorer. Autres exemples d’applications utilisant cette couche sont Office, Outlook et Skype. Toutes ces applications interactives fournissent un ensemble de services qui permettent à la couche Application de fournir des donées à recevoir des données de la couche Présentation.

La couche Présentation, ou couche 6, effectue la tâche simple du traitement de la syntaxe ou convertir des données d’un format à un autre. Par exemple, imaginez que vous commandez quelque chose dans une boutique en ligne, Ces transactions sont généralement traitées dans une transmission sécurisée ce qui signifie que les données transitant entre le « magasin » ou l4application du Site transmettra les données cryptées à la couche Présentation qui devra être déchiffré et traité. Cette couche gère la traduction des données de la couche supérieure qui est présenté sous forme de demande, au format réseau et vice versa. Une fois que la couche Présentation a traité les données d’un format à un autre, les informations sont ensuite transmises à la couche Session ou la couche Application selon que les données transmet ou reçoit.

Au niveau Session, ou couche 5, la concentruction, direction et la concluson des connexins entre les appareils se produisent. Cette couche prend en charge olusiers types de connexions ainsi que d’être responsable de l’authentification et de la reconnexion en cas d’interruption du réseau. Une fois la session établie les données passent ensuite vers ou depuis la couche Transport.

La couche Transport , ouche 4, est responsable de la transmission des données via les connexions réseau. Cette couche coordonne la quantité de données à envoyer, à quelle vitesse, ou il va, et ce genre de choses. Parmi les protocoles les plus connus pour les application Internet, ces services peuvent etre fournis par Transmission Control Protocol ou TCP et User Datagram Protocol ou UDP. D’autres protocoles peuvent fournir des capacités supplémentaires y compris la récupération d’erreurs, le flux de données et la retransmission. Une fois que la couche Transport a terminé sa fonction, les données sont ensuite transmises vers ou depuis la couche réseau.

La couche Réseau, ou couche 3, gère le routage des données. Une fois que les données arrivent à cette couche, chaque base de données est examinée pour conclure si les données ont atteint leur objectif ultime. La couche envoie les données à la bonne destination sur les transmissions sortantes et reçoit également les transmissions entrantes. La partie IP de TCP/IP est la couche réseau communément connue pour Internet. Cette couche gère également le mappage entre les adresses logiques et les adresses physiques, pour les adresses IP, ceci est accompli via le protocole de résolution d’adresse ou ARP. Les données sont ensuite transmises à la couche requise suivante qui est la couche de liaison de données.

La couche Data Link, ou couche 2, est considérée comme la plus complexe des couches. Cette couche est souvent divisée en sous-couches appelé Media Access Control ou MAC et Logical Link Control ou LLC. La couche établit des liens à travers le réseau physique. Lorsque cette couche reçoit des données de la couche Physique, il vérifie les erreurs de transmission puis regroupe les bits dans des trames de données. De là, cette couche gère les méthodes d’adressage physique pour les couches MAC ou LLC. Un exemple de la couche MAC comprend 802.11 spécifications sans fil ainsi qu’Ethernet. Au niveau de la couche de liaison de données, les données passent vers ou depuis la couche finale dans le modèle OSI qui est la couche Physique.

La couche physique, ou couche 1, est la couche électrique/physique du modèle. Cette couche comprend les câbles réseau, les prises d’alimentation, brochage des câbles, fréquences radio sans fil, connecteurs, émetteurs-récepteurs, récepteurs, répéteurs, impulsions lumineuses, tensions électriques, etc. Lors du dépannage de problèmes, c’est généralement le premier endroit pour commencer. L’appareil est-il branché ? La carte sans fil fonctionne-t-elle ? A cette couche, le modèle transmet les bits de données numériques de la source ou émetteurs Couche physique, sur les supports de communication réseau, qui peut être électrique, mécanique, ou radio, vers les dispositifs de réception ou de destination Couche physique.

Le modèle OSI est un guide pour les developpeurs et les fournisseurs pour lisser les progrès du développement de produits de communication et de logiciels qui fonctionnera en coopération avec un modèle communément établi. Une fois que vous avez compris le modèle, vous pouvez alors comprendre quels protocoles et appareils seront compatibles les uns avec les autres .

ce processus de communication peut être modéliser par une chaine composée de plusieurs maillons et la force de la chaine réside dans le maillon le plus faible .

11, 12 : Alors on va étudier une solution à cette problématique qui peut se poser comme une menace c’est la faciliter de copier le signal envoyer par la clé à