Pós-Graduação em Ciência da Computação

FÁBIO ALMEIDA MELO

SEGURANÇA EM ENTRADA E PARTIDA PASSIVAS DE AUTOMÓVEIS:

Uma revisão da literatura e um modelo

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/~posgraduacao

Recife
2019

FÁBIO ALMEIDA MELO

SEGURANÇA EM ENTRADA E PARTIDA PASSIVAS DE AUTOMÓVEIS:

Uma revisão da literatura e um modelo

Dissertação apresentada ao Programa de Pós-Graduação em Ciências da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciências da Computação.

Área de concentração: Sistemas Distribuídos.

Orientador: Prof. Dr. Carlos André Guimarães.

Recife

2019

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

M528s Melo, Fábio Almeida
Segurança em entrada e partida passivas de automóveis: uma revisão da literatura e um modelo / Fábio Almeida Melo. – 2018.
107 f.: il., fig., tab.

Orientador: Carlos André Guimarães.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2018.
Inclui referências e apêndice.

1. Ciência da computação. 2. Sistemas distribuídos. I. Guimarães, Carlos André (orientador). II. Título.

004 CDD (23. ed.) UFPE- MEI 2019-078

Fábio Almeida Melo

Segurança em Entrada e Partida Passivas de Automóveis: Uma Revisão da Literatura e um Modelo

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em: 13/09/2018.

BANCA EXAMINADORA

Prof. Dr. Abel Guilhermino da Silva Filho
Centro de Informática /UFPE

Prof. Dr. Rogério Patrício Chagas do Nascimento
Departamento de Computação/UFS

Prof. Dr. Carlos André Guimarães Ferraz
Centro de Informática / UFPE
(**Orientador**)

AGRADECIMENTOS

Agradeço ao meu orientador, à minha namorada, à minha família e a todos que contribuíram direta ou indiretamente na dissertação.

RESUMO

No começo da indústria automobilística, os veículos eram basicamente constituídos de sistemas mecânicos. Dentre esses sistemas, estavam não só sistemas como o de frenagem e aceleração, como também, o sistema antifurto, que era composto por uma simples chave mecânica. Porém, o uso da chave mecânica tornava os automóveis sujeitos a furtos por meio da duplicação das chaves ou arrombamento da fechadura. Dado o crescente número de furto de veículos, especialmente nas grandes cidades, e o advento da eletrônica, a indústria automobilística introduziu nos veículos os sistemas de entrada remota sem chaves ou RKE (Remote Keyless Entry) em meados dos anos 80. No entanto, os primeiros sistemas de RKE acrescentariam apenas mais comodidade do que segurança propriamente dita, pois eram facilmente clonados e não evitavam técnicas comuns de roubo de carro a partir da “ligação direta” no sistema de ignição. Desta forma, com o objetivo de diminuir o número de roubo de carros, a indústria automobilística passou a utilizar sistemas imobilizadores como uma proteção extra ao sistema de ignição. Em 1995, esses sistemas passariam a se tornar obrigatórios em veículos fabricados na União Europeia, medida que foi seguida por países como Austrália, Nova Zelândia e Canadá. Contudo, apesar dos esforços da indústria contra os roubos de veículos, os sistemas utilizados ainda apresentaram falhas de segurança. Essa ausência de segurança nos veículos trouxe sérios problemas à indústria automotiva nos últimos anos. Estudos recentes comprovam que veículos modernos ainda podem ser abertos e ligados sem autorização do proprietário. Nesse contexto, esta dissertação propõe uma revisão da literatura que consiste em uma revisão sistemática e uma revisão exploratória sobre controle de acesso e partida sem chaves. A partir disso, propõe-se um modelo de entrada e partida sem chaves (ou PKES - Passive Keyless Entry and Start) para veículos com foco em segurança e baseados em smartphones.

Palavras-chave: Controle de acesso à veículos. Passive Keyless Entry and Start (PKES). Remote Keyless Entry (RKE). Passive Entry and Passive Start (PEPS). Imobilizador.

ABSTRACT

In the very beginning of automobile industry, vehicles were made basically of mechanical systems. Among those systems there were braking and acceleration systems, moreover, anti-theft systems in vehicles were just mechanical key. However, mechanical keys made vehicles vulnerable to theft through duplication of keys or break-in of the lock. Due to the increasing number of vehicle thefts, especially in metropoles, and besides that the advent of electronics, automakers introduced Remote Keyless Entry (RKE) systems in the vehicles. Nevertheless, the first RKE systems would only add convenience rather than security as they were easily cloned and did not avoid common car theft techniques as hot-wiring in the ignition system. Thus, aiming to reduce car thefts, automobile industry adopted immobilizer systems as an extra protection to ignition system. In 1995, immobilizers would become mandatory in vehicles manufactured in the European Union, a move followed by countries such as Australia, New Zealand and Canada. However, despite the industry's efforts against vehicle theft, the systems used still had security issues. This lack of security on vehicles has brought serious problems to automotive industry in recent years. Recent studies show that modern vehicles can still be opened and start the engine without the owner's permission. In this context, this dissertation proposes a literature review that consists of a systematic review and an exploratory review on passive entry and passive start. Furthermore, a Passive Keyless Entry System (PKES) based on smartphones is proposed focusing on security aspects.

Keywords: Vehicle access control. Passive Keyless Entry System (PKES). Remote Keyless Entry (RKE). Passive Entry and Passive Start (PEPS). Immobilizers.

LISTA DE FIGURAS

LISTA DE QUADRO

LISTA DE SIGLAS

ABAC	Attribute Based Access Control
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
BLE	Bluetooth Low Energy
COPACOBANA	Cost-Optimized Parallel Code Breaker
CRC	Cyclic Redundancy Check
DENATRAN	Departamento Nacional de Trânsito
DoS	Denial-of-Service
DST	Digital Signature Transponder
ECU	Eletronic Control Unit
GLFSR	Galois Linear Feedback Shift Register
GPS	Global Positioning System
IBAC	Identity Based Access Control

IFF	Identify Friend or Foe
LF	Low Frequency
LFSR	Linear Feedback Shift Register
MAC Address	Media Access Control Address
MITM	Man-in-the-middle
NFC	Near Field Communication
NLFSR	Non-linear Feedback Shift Register
OICA	Organisation Internationale des Constructeurs dÁutomobiles
OOB	Out of Band
PKE	Passive Keyless Entry
PKES	Passive Keyless Entry and Start
RBAC	Role Based Access Control
RC4	Rivest Cipher 4
RFID	Radio-frequency IDentification
RKE	Remote Keyless Entry

RS	Revisão Sistemática
RSA	Rivest-Shamir-Adleman
RSSI	Received Signal Strengh Indicator
SEAC	Sensor Enhanced Access Control
SIG	Special Interest Group
UHF	Ultra High Frequency
UUID	Universally Unique Identifier

SUMÁRIO

1 INTRODUÇÃO

Este capítulo relata as principais motivações para realização deste trabalho, os objetivos de pesquisa almejados e, finalmente, mostra como está estruturado o restante da presente dissertação.

1.1 CONTEXTO E MOTIVAÇÃO

Desde o advento do automóvel por volta de 1769 (ECKERMANN, 2001), com invenção do motor a vapor, bilhares de automóveis foram produzidos no mundo, sendo mais de 1,4 bilhões nos últimos vinte anos[1]. No Brasil, segundo DENATRAN (Departamento Nacional de Trânsito), são mais de 43 milhões de veículos que circulam no país[2]. Atualmente, a produção mundial de veículos ultrapassa a casa dos 100 milhões de acordo com a OICA (*Organisation Internationale des Constructeurs d'Automobiles*)[3].

Nesses aproximadamente 250 anos da existência do automóvel uma verdadeira revolução vem acontecendo. Enquanto em 1769 os primeiros veículos funcionavam com motor a vapor, em 1805 surgiram os primeiros veículos à combustão interna, seguidos, em 1885, pelos primeiros veículos com motor de combustão a gasolina até os veículos híbridos e elétricos dos dias atuais (ECKERMANN, 2001). Essa revolução, no entanto, não se deu apenas nos motores; com o advento da eletrônica e da computação, os automóveis passaram a ter várias ECUs (*Eletronic Control Unit*) e a ter em torno de 100 milhões de linhas de código de *software*, contendo até mesmo mais linhas de código que aviões e sistemas operacionais[4]. Essa revolução ofereceu aos usuários uma infinidade de novas funcionalidades que propiciaram conforto e comodidade para realizar desde funções como dirigir, que agora conta com assistentes de direção e GPS, até o diagnóstico remoto de problemas no motor.

[1] http://www.oica.net/category/production-statistics/
[2] https://g1.globo.com/carros/noticia/frota-brasileira-de-veiculos-cresce-12-em-2017-diz-sindipecas.ghtml
[3] http://www.oica.net/category/production-statistics/2017-statistics/
[4] https://www.ibm.com/blogs/internet-of-things/iot-design-for-system-of-systems/

Durante toda essa revolução, os sistemas como os de entrada e partida, que antes eram mecânicos, passariam a se tornar sistemas de entrada remota (*Remote Keyless Entry* – RKE) através do uso de rádio frequência em 1982 com o Renault Fuego[5], seguido pelo sistema de entrada passiva (*Passive Keyless Entry* – PKE) do Corvette em 1993[6] e, finalmente, com o sistema de entrada e partida passiva (*Passive Keyless Entry and Start* – PKES) do Mercedes S-Class em 1998, fazendo com que o simples ato de entrar no automóvel e liga-lo fosse possível sem precisar retirar a chave do bolso e utilizar de um simples toque em um botão para ligá-lo.

Porém, mesmo com toda essa revolução tecnológica pela qual o automóvel passou, ainda não foi o suficiente para torná-los completamente seguros do ponto de vista da tecnologia da informação. Pois junto com os avanços tecnológicos vieram novas falhas de segurança da informação e de aspectos de privacidade. Com isso, cada vez mais, quadrilhas especializadas formadas por *hackers* têm obtido sucesso em comprometer a segurança do automóvel[7]. Segundo a Interpol, mais de 36 milhões de carros foram reportados como roubados entre 2012 e 2017 em todo o mundo, isso sem contabilizar os casos não registrados[8]. Na França, cerca de 74% roubos de carros em 2015 se deram através de *hackers* e na Inglaterra, em 2014, quase metade dos roubos de carros se deram sem as chaves[9]. Recentemente, um circuito de câmeras de segurança flagrou dois assaltantes abrindo uma Mercedes-Benz em menos de um minuto sem o uso de arrombamento e chaves[10], o mesmo aconteceu com uma BMW[11] e uma Land Rover Discovery[12].

Apesar de recentes, esses ataques apenas corroboram com o que já vem sendo propagado há anos pela comunidade científica. Diversos estudos têm demonstrado ao longo de tempo a fragilidade dos sistemas de entrada e partida em termos de segurança. Em (BONO et al., 2005), a análise do Digital Signature Transponder da Texas Instruments evidenciou uma falha no tamanho da chave que afeta mais de 150 milhões de veículos. Já o Keeloq, que é utilizado por diversos modelos da Volvo, Toyota, Honda e Fiat, teve falhas expostas em diversos trabalhos (COURTOIS;

---

[5] https://www.motor1.com/news/131217/worst-sports-cars-renault-fuego/
[6] https://www.corvsport.com/1993-c4-corvette/
[7] https://www.bbc.com/news/technology-29786320
[8] https://www.interpol.int/Crime-areas/Vehicle-crime/Database-statistics
[9] https://www.telegraph.co.uk/news/worldnews/europe/france/11964140/Three-quarters-of-cars-stolen-in-France-electronically-hacked.html
[10] https://www.express.co.uk/life-style/cars/885216/relay-car-theft-keyless-entry-advice-faraday-cage
[11] https://www.express.co.uk/life-style/cars/866987/car-theft-hack-keyless-entry-video-BMW-stolen
[12] https://www.bbc.com/news/av/uk-england-birmingham-40979096/land-rover-discovery-stolen-in-solihull-in-keyless-theft

O'NEIL; QUISQUATER, 2009; EISENBARTH et al., 2008; INDESTEEGE et al., 2008; MALAGÓN et al., 2015; PAAR et al., 2009; SHEETRIT; WOOL, 2011). Em Verdult, Garcia e Balasch (2012) os ataques demonstram a fragilidade do Hitag2, que é utilizado em mais de 200 modelos de 34 montadoras. Esse estudo, demonstrou que o Hitag2 pode ser *hackeado* em menos de 360 segundos. Já Wang e Yu (2005), informa que o Megamos Crypto que, segundo o fabricante, teve mais de 100 milhões de dispositivos produzidos, é explorado através de 3 ataques. Em outro importante estudo, Garcia et al. (2016) expõem falhas do RKE utilizado pelo Grupo Volkswagen, que é um dos líderes mundiais na produção de veículos, atingindo modelos como Fox, Golf, Audi A1, Audi Q3, entre outros.

Assim, diante dessa problemática crescente de roubos de veículos, em especial as que ocorrem através do comprometimento dos sistemas de entrada e partida sem chaves, também conhecido como entrada e partida passivas (*Passive Keyless Entry and Start* – PKES), esse trabalho busca apresentar o que de mais importante tem sido pesquisado pela indústria e academia em relação à segurança dos PKES e, diante do levantado na literatura, propor um modelo composto por partes das propostas consideradas mais seguras, considerando o uso de um smartphone como chave virtual do PKES.

1.2 OBJETIVOS

Essa dissertação tem como objetivo apresentar o que vem sendo pesquisado pela academia e indústria através da realização de uma revisão da literatura sobre entrada e partida em automóveis. Além disso, a partir dos resultados obtidos pela revisão, um outro objetivo desse trabalho é a elaboração de um sistema de controle de acesso e partida sem chaves em veículos baseado em *smartphones* com foco em segurança da informação. Para alcançar esse objetivo, análise dos trabalhos encontrados na literatura e dos sistemas existentes no mercado é de suma importância, uma vez que o modelo proposto é composto por soluções encontradas nesta revisão da literatura.

1.3 ESTRUTURA DA DISSERTAÇÃO

Daqui em diante este trabalho está estruturado da seguinte maneira:

- **Capítulo 2 – Referencial Teórico:** O segundo capítulo tem como objetivo apresentar conceitos fundamentais utilizados em sistemas de entrada e partida passivas sem chaves.
- **Capítulo 3 – Revisão da Literatura:** Nesse capítulo é apresentado como foi realizada a revisão da literatura. Inicialmente é apresentada a revisão

sistemática e em seguida a revisão exploratória. Além disso, os resultados obtidos na revisão sistemática e na exploratória também são apresentados, incluindo os principais requisitos analisados. O Capítulo 3 também apresenta os ataques e as vulnerabilidades dos principais sistemas encontrados na literatura.

- **Capítulo 4 – Modelo Proposto**: O quarto capítulo apresenta um modelo de controle de acesso e partida sem chaves baseado em smartphones e com foco em segurança, elaborado a partir da revisão da literatura.
- **Capítulo 5 – Considerações Finais:** O último capítulo encerra a dissertação apresentando as principais conclusões, os resultados obtidos, as limitações e sugestões de trabalhos futuros, visando a dar continuidade à pesquisa realizada por esse trabalho.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os conceitos fundamentais sobre as tecnologias envolvidas no desenvolvimento do modelo proposto.

2.1 ENTRADA E PARTIDA EM VEÍCULOS

Os primeiros veículos que se tem conhecimento com sistema de entrada e partida faziam uso de sistemas mecânicos com o uso de chaves mecânicas. Porém, os veículos eram facilmente violados ou podiam ter as chaves copiadas. A partir de 1982, o primeiro RKE (*Remote Keyless Entry* – Entrada Remota sem Chave) foi introduzido através do Renault Fuego[13]. Os RKEs permitiram aos usuários travar e destravar as portas do veículo com apenas um clique de um botão em um controle remoto. Para isso, as chaves, que antes eram mecânicas, passaram a contar com dispositivos eletrônicos providos de antenas para enviar comandos e se comunicar com o automóvel. Porém, os primeiros RKE trariam mais conforto que segurança, propriamente dito. Com o crescente aumento do número de roubos de carros, a indústria automobilística passou a adotar sistemas imobilizadores como uma proteção extra ao sistema de ignição. Em 1995, esses sistemas passariam a se tornar obrigatórios em veículos fabricados na União Europeia (EC, 1995), medida que foi seguida por países como Austrália, Nova Zelândia e Canadá (AS/NZS, 1999; SCC, 1998). Ainda na década de 1990, através do 1993 C4 Corvette, o primeiro PKE (*Passive Keyless Entry* – Entrada Passiva sem Chave) era introduzido no mercado automobilístico. No entanto, ainda era necessária a chave para dar partida ao automóvel[14]. Anos depois, em 1998, a Mercedes-Benz introduzia no mercado, através do Mercedes S-Class, o Keyless-Go produzido pela Siemens que é considerado o primeiro PKES (*Passive Keyless Entry and Start* – Entrada e Partida Passiva sem Chave).

Com os PKES, os usuários passaram a travar e destravar as portas do veículo apenas ao se aproximar ou se afastar do veículo com a chave próxima ao corpo como, por exemplo, dentro do bolso. Para que isso fosse possível, os veículos foram equipados com antenas que, junto com técnicas de localização como, por exemplo, a

[13] https://www.motor1.com/news/131217/worst-sports-cars-renault-fuego/
[14] https://www.corvsport.com/1993-c4-corvette/

triangulação, conseguem detectar a presença da chave nas proximidades ou dentro do veículo.

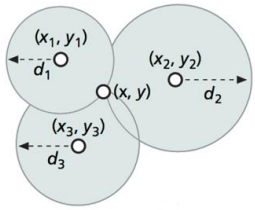
Atualmente, alguns modelos de luxo como, por exemplo, o BMW série 3 também possuem um chip de telefonia móvel para travamento e destravamento remoto de portas através de um aplicativo no celular (BMW, [s.d.]). Além disso, fabricantes de equipamentos estão desenvolvendo PKES que utilizam o *smartphone* como chave virtual para os veículos (BOSCH, [s.d.]; CONTINENTAL, [s.d.]).

2.2 LOCALIZAÇÃO

Existem diversas maneiras de se localizar um dispositivo em ambientes *indoor* e *outdoor*. As principais formas de estimativas de distância se baseiam em: força de sinal recebido (*Received Signal Strength Indicator* - RSSI), tempo de chegada (*time-of-arrival* e *time-difference-of-arrival*) e ângulo de chegada (*angle-of-arrival*). Então, diante desses valores, pode-se estimar a localização através de algum método, dentre os quais estão a trilateração hiperbólica, a triangulação e o *bounding box* (BOUKERCHE; NAKAMURA, 2007).

- Na trilateração hiperbólica a localização é dada a partir do cálculo da interseção de três círculos.

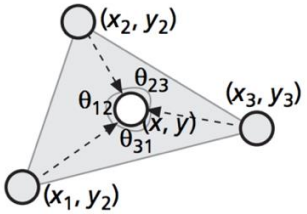
Figura 1 - Trilateração hiperbólica



Fonte: Boukerche & Nakamura (2007**)**

- Na triangulação, as propriedades geométricas do triângulo são utilizadas para estimar a posição.

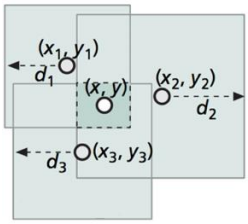
Figura 2 - Triangulação



Fonte: Boukerche & Nakamura (2007)

- No *bounding box* a localização é dada a partir da intersecção de três quadrados.

Figura 1 - *Bounding box*



Fonte: Boukerche & Nakamura (2007)

Atualmente diversos estudos têm sido feitos em localização *indoor* e *outdoor* com redes sem fio (CHAI; AN; DU, 2016; JIANYONG et al., 2014; KALBANDHE; PATIL, 2016, 2016; SADOWSKI; SPACHOS, 2018; THALJAOUI et al., 2015; WANG et al., 2016).

2.3 COMUNICAÇÃO SEM FIO

Dentro das possibilidades de comunicação sem fio adotadas para um sistema baseado em *smartphones* (sem uso de hardware adicional) podemos citar o Bluetooth, BLE (*Bluetooth Low Energy*), e NFC (*Near Field Communication*). Além dessas redes, poderíamos incluir a Wifi e o 3G/4G, porém, essas redes possuem algumas limitações que as tornam inadequadas para o uso em um PKES. Enquanto a Wifi tem como impeditivo o tempo para estabelecer uma conexão (PEI et al., 2017). Já as redes de celulares têm um custo mais elevado, pois necessitariam de uma operadora de telefonia ou de uma licença para operar na faixa de frequência.

2.3.1 Bluetooth

O padrão bluetooth foi desenvolvido pelo grupo de interesse (Special Interest Group - SIG) inicialmente composto por cinco empresas; Ericsson, IBM, Intel, Nokia e Toshiba, e que atualmente, encontra-se na versão 5.0 (BLUETOOTH SPECIAL INTEREST GROUP (SIG), 2016). O Bluetooth foi criado com o objetivo de se tornar um padrão de comunicação sem fio aberto de curto alcance e de baixa potência. O Bluetooth opera na faixa de frequência de 2.4 GHz e tem taxas de transferência de dados de até 2.1 Mbit/s e um alcance de até 100 metros. Além disso, para realizar a conexão (pareamento) entre dois dispositivos o Bluetooth pode levar até 6 segundos (BLUETOOTH SPECIAL INTEREST GROUP (SIG), 2016).

De acordo com a especificação (BLUETOOTH SPECIAL INTEREST GROUP (SIG), 2016), existem 4 formas de realizar o pareamento entre dois dispositivos bluetooth: Just Works, Numeric Comparison, Passkey Entry e Out of Band (OOB). No primeiro, não há autenticação e os dispositivos se conectam sem interação do usuário, em alguns casos pode haver necessidade de confirmar se o usuário deseja se conectar. No segundo, os usuários precisam confirmar se os 6 dígitos que aparecem

no visor de cada dispositivo coincidem. No método Passkey Entry, uma senha de 6 dígitos precisa ser digitada para realizar o pareamento. Por último, no OOB algum mecanismo externo ao bluetooth é usado para trocar informações, normalmente é usado NFC (Near Field Communication).

2.3.1.1 *Bluetooth Low Energy*

Introduzido pela primeira vez no Bluetooth 4.0 (BLUETOOTH SPECIAL INTEREST GROUP (SIG), 2016) e aperfeiçoado em versões seguintes, o Bluetooth Low Energy (BLE) tem como principais características a conexão rápida, menor taxa de transferência de dados, um menor alcance e um menor consumo de energia se comparado à implementação do Bluetooth. Devido ao baixo consumo de energia, ele é apontado como uma das tecnologias-chave para comunicação sem fio na Internet das Coisas (BORGIA, 2014). Ao contrário do Bluetooth clássico, o BLE tem alcance de até 50m e uma taxa de transferência de 1 Mbit/s. Por outro lado, o BLE leva 0,006s para conexão e consome menos energia.

2.3.2 NFC

Near Field Communication (NFC) é um padrão de tecnologia sem fio voltada para troca de dados em curtíssimo alcance (menos de 20 centímetros) que opera em uma faixa de frequência de 13,56 MHz e com taxas de transferência de até 424 Kbit/s (AL-SARAWI et al., 2017).

2.3.3 Análise Comparativa

Diante da possibilidade de uso das três redes para uma aplicação de PKES baseada em smartphones, o Quadro 2 apresenta um comparativo entre elas.

Quadro 1 - Comparativo NFC x Bluetooth x BLE **(**

	NFC	Bluetooth	BLE
Alcance	< 20 cm	~ 100 m (classe 1)	~ 50 m
Frequência	13,56 MHz	2,4-2,5 GHz	2,4-2,5 GHz
Transmissão	424 Kbit/s	2,1 Mbit/s	1 Mbit/s
Tempo de conexão	< 0,1s	< 6s	< 0,006s
Corrente	15 mA	30 mA	15 mA

Fonte: Adaptada de AL-SARAWI et al. (2017) e GOMEZ; OLLER; PARADELLS (2012)

Nota-se que o tempo de conexão entre dispositivos Bluetooth clássico é muito grande, já para NFC e BLE os valores são bem menores. Um outro fator importante é a distância em que as tecnologias funcionam, tendo o NFC um campo de ação muito restrito.

2.4 COMPUTAÇÃO SENSÍVEL AO CONTEXTO

O termo contexto em computação possui diversas definições, sendo a mais clássica a que foi definida por Dey: "qualquer informação que pode ser usada para caracterizar a situação de uma entidade. Uma entidade é uma pessoa, lugar ou objeto que é considerado relevante para a interação entre um usuário e uma aplicação, incluindo o próprio usuário e as próprias aplicações" (DEY, 2001), e esse contexto geralmente está relacionado a dados sobre a localização, a identidade e o estado de entidades ou grupos de entidades.

Dey vai além e define que um sistema sensível ao contexto é aquele que "usa o contexto para fornecer informações e/ou serviços relevantes para o usuário, onde a relevância depende da tarefa do usuário" (DEY, 2001). Essa definição de contexto e consciência de contexto[15] resulta em sistemas que melhoraram sua eficiência e experiência do usuário pelo uso inteligente de informações contextuais.

Em termos de segurança, a computação sensível ao contexto pode ser utilizada como um fator de autenticação em sistemas em que a autenticação ocorre em mais de um passo. Em Bardram, Kjær e Pedersen (2003), tem-se um sistema hospitalar na qual o *login* do usuário no sistema acontece através de informações contextuais de localização. Já no trabalho de Covington et al. (2002), informações contextuais são capturadas através de vários sensores distribuídos em uma casa e utilizados na autenticação e autorização para, por exemplo, impedir que uma criança assista televisão a partir de onze da noite. Já em AL-Muhtadi et al. (2003) é apresentado o Cerberus, um sistema de autenticação e autorização ciente de contexto. Em Truong et al. (2015), é apresentado um sistema para bloquear e desbloquear um computador a partir de informações contextuais que indicam a presença do usuário. Em Iatrou (2017), é definido o SEAC (*Sensor Enhanced Access Control*), que através de câmeras e um algoritmo de rastreamento, autentica e autoriza pessoas para utilizar o sistema de arquivos de um *desktop*.

2.5 ATAQUES EM SISTEMAS DE ENTRADA E PARTIDA

Esta seção aborda alguns dos ataques a sistemas de entrada e partida existentes na literatura.

2.5.1 Força Bruta

Esse ataque se aproveita do tamanho da chave e realiza diversas combinações com tentativas de autenticação até que a chave utilizada seja encontrada. Na

[15] Também conhecido como “ciência de contexto” ou “sensível a contexto”.

literatura, existem diversas técnicas para realizar o ataque, entre elas a busca exaustiva, que realiza todas as tentativas possíveis, e o *time-memory-tradeoff*, que pré-computa tabelas de dados com possíveis chaves para diminuir o tempo de processamento de gerar todas as chaves possíveis (BORST; PRENEEL; VANDEWALLE, 1998).

2.5.2 Jamming

Em redes sem fio, esse ataque consiste em gerar sinais de ruído na mesma frequência em que a comunicação acontece com o objetivo de impedir a comunicação. (XU et al., 2006)

2.5.3 Man-in-the-middle

No ataque *man-in-the-middle* (MITM), o atacante intercepta a comunicação entre carro e chave para capturar as mensagens trocadas entre eles. Essa interceptação pode ser realizada com o intuito de aprender sobre o sistema, retransmitir as mensagens ou adulterar e retransmitir as mensagens (WELCH; LATHROP, 2003).

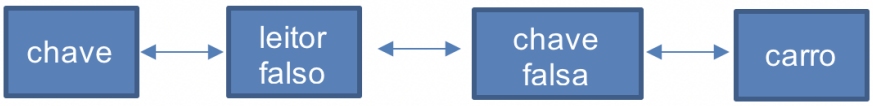
2.5.4 Replay Attack

Esse ataque é um tipo de MITM que consiste em interceptar mensagens para uso futuro (WELCH; LATHROP, 2003). As mensagens interceptadas são retransmitidas e podem ou não ser adulteradas. Para efetuar o ataque é preciso interceptar a comunicação através do MITM e ter algum conhecimento do formato das mensagens existentes no protocolo no caso de alguma adulteração.

2.5.5 Relay Attack

Esse ataque tem se tornado uns dos principais ataques em PKES (FRANCILLON; DANEV; CAPKUN, 2011). Por não necessitar de interação humana para autenticar, o atacante se posiciona entre a chave e o veículo para iniciar a comunicação entre eles e retransmitir a mensagem de ambos. Para isso ele introduz uma chave falsa e um leitor (veículo) falso com sinais amplificados, então veículo e chave autênticos se comunicam acreditando que se trata da chave e do leitor reais (Figura 4) (TILLICH; WÓJCIK, 2012). Esse ataque pode ser considerado uma versão do MITM.

Figura 2 - Relay Attack



Fonte: Tillich & Wójcik (2012)

2.5.6 Cryptanalysis

Esse ataque está relacionado à fragilidade do algoritmo de criptografia utilizada. Através da análise do algoritmo, esse ataque pode ser combinado com outro ataque, por exemplo, MITM para obter a chave a partir de poucas mensagens interceptadas. Um tipo de ataque de cryptanalysis é o *Algebraic attack*, que reduz a complexidade das funções lineares dos cifradores de fluxo ao transformar o cifrador em um sistema de equações (COURTOIS, 2003).

2.5.7 Side Channel attack

Um *side channel attack* é um ataque que obtém vantagem de quaisquer informações vazadas durante a execução de um processo de criptografia (OKEYA; SAKURAI, 2002). Essas informações podem ser: análise de memória *cache*, consumo de energia, análise diferencial de falhas (do inglês, *Differential Fault Analysis* – DFA).

2.5.8 Denial of Service

O ataque de *denial of service* consiste em inutilizar o sistema que está sendo atacado (WOOD; STANKOVIC, 2004). Em sistemas de entrada e partidas, esse ataque pode ser realizado através de envio de mensagens com contadores fora da janela esperada pelo veículo. Para isso, pode ser utilizada uma combinação do MITM para interceptar mensagens e em seguida retransmitir mensagens com contadores antigos (*replay attack*) (GARCIA et al., 2016) ou corrompendo a memória da chave ou do automóvel .

2.6 SEGURANÇA

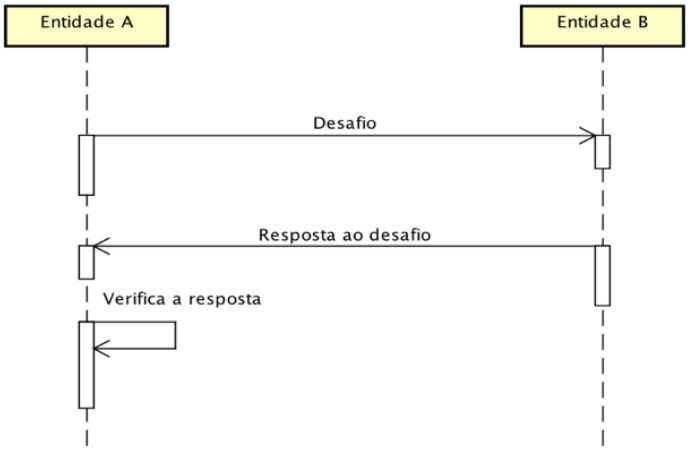
Em sistemas de PKES, a segurança é um dos principais fatores a ser considerado ao projetar um sistema. Além disso, devido ao fato desses sistemas usarem a comunicação sem fio, várias medidas precisam ser tomadas, dado que a informação trafega livremente pelo meio e qualquer um pode intercepta-la. As subseções a seguir apresentam abordagens que podem ser utilizadas para mitigar problemas de segurança em PKES.

2.6.1 Autenticação

Para evitar que qualquer pessoa tenha acesso ao veículo, os sistemas de controle de entrada e partida fazem uso da autenticação. A autenticação é realizada através de algoritmos de criptografia e garantem uma prova de autenticidade entre as entidades. No contexto de PKES, existem basicamente dois tipos de autenticação: unilateral e mútua (bilateral). Eles se baseiam no fato de que somente usuários que conhecem a chave compartilhada conseguirão responder a um desafio.

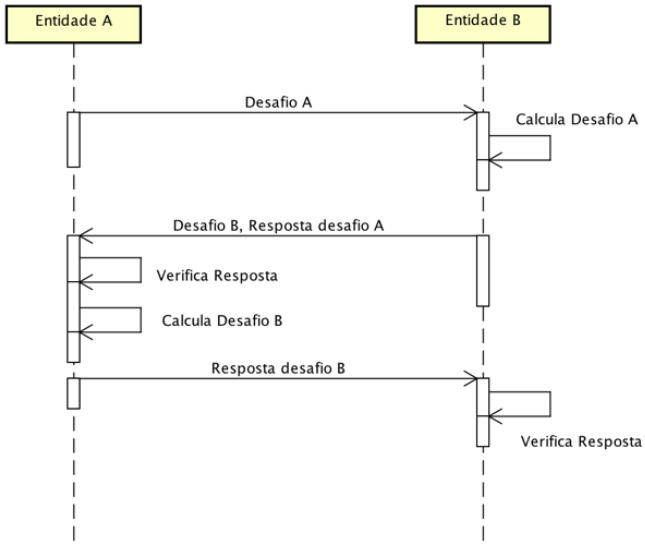
Na autenticação unilateral, apenas uma das entidades envolvidas prove legitimidade a outra (Figura 5). Já na autenticação mútua, ambas as entidades provêm legitimidade (Figura 6).

Figura 3 - Autenticação unilateral



Fonte: O autor (2019)

Figura 4 - Autenticação mútua



Fonte: O autor (2019)

2.6.2 Autorização

Além da autenticação, uma outra técnica utilizada para controle de acesso em sistemas é a autorização. Diferentemente da autenticação que decide se um usuário tem ou não acesso a um sistema, a autorização determina o que um usuário autenticado pode fazer no sistema. Na literatura existem diversos modelos de controle de acesso, dentre os quais estão o Identity Based Access Control (IBAC), o Role Based Access Control (RBAC) e o Attribute Based Access Control (ABAC).

No IBAC as permissões aos recursos do sistema estão associados a um identificador do usuário (YUAN; TONG, 2005). Um exemplo do IBAC são as Access Control Lists (ACL) utilizadas em sistemas operacionais. A grande vantagem desse paradigma é a sua fácil implementação, porém ele não é facilmente escalável à medida que a quantidade de identificadores de um recurso cresce (YUAN; TONG, 2005).

No paradigma RBAC cada usuário tem um papel associado (ex.: proprietário de veículo) e os acessos a certos recursos do sistemas estão restritos a esse papel (YUAN; TONG, 2005). A grande vantagem do RBAC é que os papéis são facilmente associados às regras de negócio da aplicação, porém não há como diferenciar usuários com o mesmo papel.

Já o ABAC é um paradigma de controle de acesso que garante permissão aos usuários através de combinações de atributos (FISHER et al., 2016). De acordo com (YUAN; TONG, 2005), os atributos podem ser entidades que realizam uma ação (um usuário, um processo, etc.), uma entidade que sofre uma ação (um componente do sistema, um serviço web, etc.) ou algum atributo de ambiente (data, hora, nível de segurança da rede, etc.). De acordo com (FISHER et al., 2016), o ABAC permite um controle de acesso mais refinado que o RBAC, uma vez que ele consegue traduzir regras de negócios em políticas baseadas em atributos.

2.6.3 Whitelist e Blacklist

Em termos de servidores, a técnica de *whitelist* consiste em uma lista de endereços aos quais o acesso a um determinado serviço é permitido. Já a *blacklist*, é uma lista com os endereços que não possuem acesso a um serviço (GUARD, 2013). Ambas as técnicas podem ser utilizadas para mitigar ataques de *denial of service*, uma vez que elas impedem que usuários indesejados tenham acesso ao serviço.

2.6.4 Criptografia

Um meio bastante utilizado para proteger a comunicação sem fio é a criptografia. A criptografia protege privacidade do conteúdo das mensagens trocadas em uma rede mesmo que a conversa seja interceptada. Segundo Simmons (1979), a criptografia pode ser dividida em dois grupos de algoritmos: simétricos e assimétricos. Algoritmos simétricos são aqueles onde a chave para criptografar e descriptografar mensagens é a mesma. Já nos algoritmos assimétricos uma chave é utilizada para criptografar e outra, utilizada para descriptografar. Existem diversos algoritmos assimétricos na literatura, entre eles Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DAS)

e Diffie-Hellman. Já entre os algoritmos simétricos, podemos citar o Advanced Encryptation Standard (AES), Rivest Cipher 4 (RC4) e o Blowfish.

Dentro dos algoritmos simétricos existem os cifradores de blocos (*block ciphers*) e os cifradores de fluxo (*stream ciphers*) (ROB, 1982). Os cifradores de blocos funcionam com blocos de tamanho fixo e a saída do processo de criptografia depende diretamente do próprio dado a ser criptografado - uma simples mudança no dado pode mudar completamente o resultado da criptografia. Já os cifradores de fluxo operam bit por bit, gerando um texto cifrado a partir de dados secretos combinado com dados aleatórios. Existem dois tipos de cifradores de fluxo: síncronos e auto-sincronizáveis (ROB, 1982). No primeiro, a criptografia dos bits independe do texto a ser cifrado. Já nos auto-sincronizáveis, o cifrador computa o estado interno atual a partir do estado anterior e do texto cifrado.

3 REVISÃO DA LITERATURA

Este capítulo descreve o método científico utilizado nesse estudo. A descrição do método detalha como foram obtidos os resultados e quais foram esses resultados. Esse capítulo foi divido em seções para facilitar a compreensão das etapas do processo.

3.1 INTRODUÇÃO

De modo a realizar uma revisão ampla da literatura, esse trabalho utilizou-se de um método de pesquisa conhecido como Revisão Sistemática (RS). Além disso, para aumentar a abrangência dessa revisão e devido ao fato da pesquisa também abranger questões de mercado, também foi realizada uma Revisão Exploratória.

Segundo (BUDGEN; BRERETON, 2006), uma RS é uma forma de estudo que propõe uma metodologia bem definida para identificar, interpretar e analisar evidências de maneira imparcial e replicável. Essas evidências são elaboradas a partir da seleção e síntese de pesquisas relevantes para um campo de pesquisa. A Revisão Sistemática foi realizada em duas etapas: uma revisão sistemática da literatura e uma revisão sistemática de patentes.

Já as revisões exploratórias não possuem um método ou processo bem definidos (POLLITT, 2007), mas são importantes para incluir trabalhos publicados em meios não acadêmicos como, por exemplo, relatórios técnicos e produtos de empresas.

As Seções 3.2, 3.3 e 3.4 deste capítulo explicam como foram realizadas as revisões, a Seção 3.5 consolida os resultados das revisões. A Seção 3.6 analisa alguns dos requisitos de PKES (do inglês, *Passive Keyless Entry and Start*) e a Seção 3.7 e 3.8 analisam vulnerabilidades e ataques aos sistemas. Por último, a Seção 3.9 faz as considerações finais do capítulo.

3.2 REVISÃO SISTEMÁTICA DA LITERATURA

O objetivo dessa Seção é explicar o procedimento realizado na Revisão Sistemática da Literatura desse trabalho.

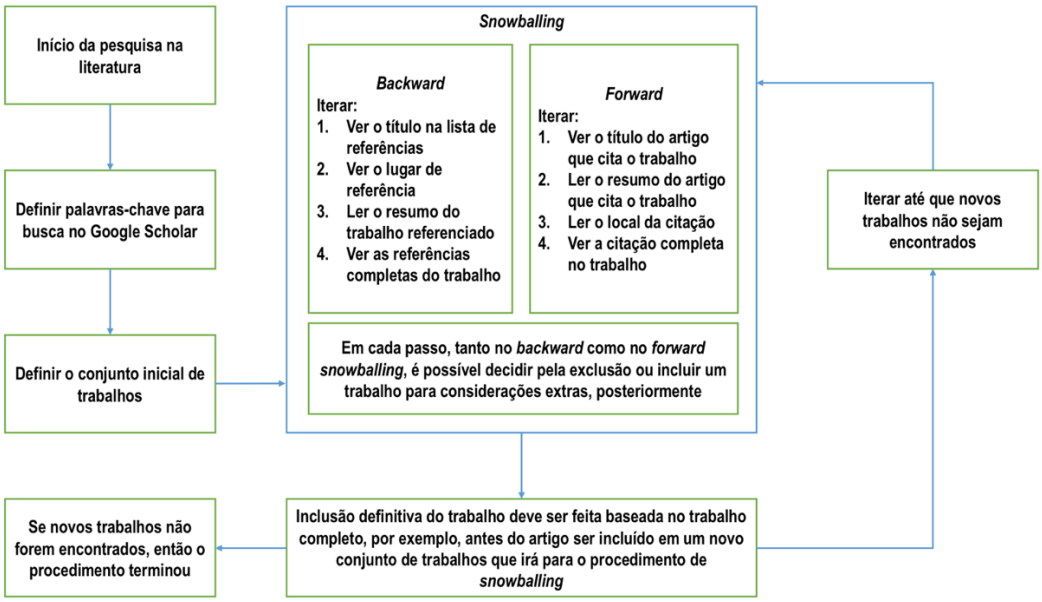
3.2.1 Metodologia

A técnica usada para essa revisão da literatura foi a de *forward* e *backward snowballing*. Essa técnica consiste em pesquisar todos os artigos que fazem referência a um artigo de um conjunto de artigos (*forward snowballing*) e pesquisar entre todas as referências feitas nesse conjunto de artigos (*backward snowballing*). A escolha dessa abordagem foi apoiada pelo trabalho de (JALALI; WOHLIN, 2012). Nesse trabalho, uma comparação entre busca por palavras-chave e *backward snowballing* é realizada, no qual chega-se à conclusão de que não há grande diferença nos resultados alcançados entre as metodologias usadas. Porém, a metodologia de *backward snowballing* é mais eficiente do que a busca por palavras-chave quando os termos de busca utilizados são muito comuns, o que é o caso do trabalho em questão, onde as palavras-chave são "*car*", "*security*", "*keyless entry*", entre outras.

Na comparação feita em (JALALI; WOHLIN, 2012), a busca por palavras-chave obteve um ruído (artigos que não eram de interesse da pesquisa) de 85%, enquanto a *backward snowballing* obteve um ruído de apenas 32%, tornando-a mais eficiente. Jalali e Wohlin, em seu trabalho, ainda recomendam que seja feito não só o *backward snowballing*, como também o *forward snowballing*.

Então, a partir das conclusões do trabalho de (JALALI; WOHLIN, 2012), foi realizada uma revisão da literatura baseada no trabalho de (WOHLIN, 2014). Nesse trabalho, Wohlin define de maneira sistemática um passo a passo para a execução de uma revisão sistemática utilizando-se da técnica de *forward* e *backward snowballing*. As próximas subseções definem o passo a passo realizado (Figura 7), e os resultados preliminares encontrados.

Figura 7 - Revisão sistemática



Fonte: adaptada de Wohlin (2014)

3.2.2 Critérios de Elegibilidade

Para que um artigo seja incluído na revisão sistemática, foram estabelecidos os seguintes critérios de elegibilidade:

- Artigos escritos em inglês;
- Trabalhos publicados entre Janeiro de 2007 e Setembro de 2018;
- Local de publicação do artigo;
- Artigos que envolvam segurança nos sistemas veiculares de entrada e partida sem chaves;
- Relevância do artigo na área da pesquisa;

Vale ressaltar que os artigos que já foram selecionados em uma etapa anterior não são incluídos nas etapas seguintes.

3.2.3 Seleção do Conjunto Inicial de Artigos

Para definição do conjunto inicial de artigos foi feita uma busca por palavras-chave no Google Scholar. As palavras-chave utilizadas foram: "*car*", "*keyless entry*" e "*security*". Essa busca foi realizada por dois pesquisadores, e então, os dez principais artigos que pertencia à lista de ambos os pesquisadores com mais citações (de acordo com o Google Scholar) foram selecionados como o conjunto inicial. Esses artigos obedecem aos critérios de elegibilidade estabelecidos na Seção anterior. De acordo com Wohlin (2014), o uso do Google Scholar evita um viés na pesquisa, pois ele indexa as principais bases de pesquisa como IEEE, ACM, Science Direct, Springer, entre outras. Ainda segundo Wohlin, um bom conjunto inicial de artigos não deve ser pequeno e deve ser bem diversificado em termos de autores, anos de publicação e

fontes científicas. Então, como conjunto inicial foram escolhidos os seguintes artigos do Quadro 2.

Quadro 2 - Conjunto inicial de artigos

Título	Autor(es)	Publicação	Ano
A practical attack on KeeLoq	Indesteege, S., Keller, N., Dunkelman, O., Biham, E., and Preneel, B.	EUROCRYPT	2008
On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme	Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M. T. M., et al.	CRYPTO	2008
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars	Francillon, A., Danev, B., and Capkun, S.	Annual Network and Distributed System Security Symposium	2011
Gone in 360 Seconds - Hijacking with Hitag2	Verdult, R., Garcia, F. D., and Balasch, J.	USENIX	2012
Dismantling Megamos Crypto - Wirelessly Lockpicking a Vehicle Immobilizer	Verdult, R., Garcia, F. D., and Ege, B.	USENIX	2013
Broken keys to the kingdom Security and privacy aspects of RFID-based car keys	Wetzels, J	Seminar Information Security Technology - Kerckhoffs Institute	2014
Cryptanalysis of the Megamos Crypto Automotive Immobilizer	Verdult, R. and Garcia, F. D.	USENIX	2015
Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems	Garcia, F. D., Oswald, D., Kasper, T., and Pavlid`es, P	USENIX	2016
A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography	Glocker, T., Mantere, T., and Elmusrati, M.	Int. Conference on Information and Communication Systems	2017
One Car, Two Frames-Attacks on Hitag-2 Remote Keyless Entry Systems Revisited	Benadjila, R., Renard, M., Lopes-Esteves, J., and Kasmi, C.	USENIX	2017

Fonte: O autor (2019)

3.2.4 Iterações de backward e forward snowballing

No caso de iterações de *forward snowballing,* os trabalhos que referenciam os artigos do conjunto inicial são analisados. Já no caso de *backward snowballing,* são avaliadas todas as referências dos artigos do conjunto inicial.

Para facilitar a análise, primeiramente o pesquisador verifica se o ano de publicação do artigo está entre as datas pré-estabelecidas, em seguida observa o título e o *abstract* do artigo em análise. Caso o artigo se inclua nos critérios de elegibilidade e não tenha sido selecionado anteriormente, ele é incluindo no conjunto de artigos para a iteração seguinte, caso contrário, ele é descartado.

3.2.5 Primeira Iteração

Na primeira iteração são avaliados os artigos do conjunto inicial definido no Quadro 2.

3.2.5.1 *Forward Snowballing*

Na primeira iteração de *forward snowballing* foram incluídos 21 novos artigos. A inclusão ou exclusão dos artigos seguem os critérios de elegibilidade definidos na seção 3.2.2. Os artigos estão listados na Quadro 3.

Quadro 3 - Trabalhos selecionados na primeira iteração de *forward snowballing* **(continua)**

Título	Autor(es)	Publicação	Ano
Bitslice software implementation of KeeLoq as a side-channel countermeasure	Malagón et. al	Workshop on Embedded Systems Security	2015
Cryptanalysis of KeeLoq code-hopping using a Single FPGA	Sheetrit, I. e Wool, A.	IACR Cryptology	2011
Exploiting bit-level parallelism in GPGPUs: A case study on KeeLoq exhaustive key search attack	Agosta et. al	International Conference On Architecture of Computing Systems	2012
Passive keyless entry system for long term operation	Oguma et. al	IEEE Int.Symposium on a World of Wireless, Mobile and Multimedia Networks	2011
Periodic ciphers with small blocks and cryptanalysis of keeloq	Courtois et. al	Tatra Mt. Math. Publ	2008
Self-similarity Attacks on Block Ciphers and Application to KeeLoq	Courtois, N. T.	Cryptography and Security: From Theory to Applications	2012
Towards a distributed secure in-vehicle communication architecture for modern vehicles	Patsakis et. al	Computers & Security	2014
Vehicle Relay Attack Avoidance Methods Using RF Signal Strength	Kim et. al	Communications and Network	2013
Clone-resistant vehicular RKE by deploying SUC	Hamadaqa et. al	Int. Conference on Emerging Security Technologies	2017

Quadro 4 - Trabalhos selecionados na primeira iteração de *forward snowballing* **(conclusão)**

Título	Autor(es)	Publicação	Ano
Key Is In The Air: Hacking Remote Keyless Entry Systems	Ibrahim et. al	-	2018
Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System	Choi et. al	Journal of Advanced Transportation	2018
Designing wireless automotive keys with rights sharing capabilities on the MSP430 microcontroller	Groza et. al	International Conference on Vehicle Technology and Intelligent Transport Systems	2017
An Automobile Security Protocol: Side-channel Security against Timing and Relay Attacks	Isa et. al	Int. Journal of Electronic Security and Digital Forensics	2017
Channel correlation-based relay attack avoidance in vehicle keyless-entry systems	Jeong, H. e So, J.	IEEE Eletronic letters	2018
Breaking a Hitag2 Protocol with Low Cost Technology	Stembera, P. e Novotny, M.	Euromicro Conference on Digital System Design	2017
Hitag 2 Hell – Brutally Optimizing Guess-and-Determine Attacks	Verstegen et. al	USENIX	2018
AuthentiCap - A Touchless Vehicle Authentication and Personalization System	Franl, S.	European Conference on Ambient Intelligence	2017
A Smart Wireless Car Ignition System for Vehicle Security	Haider et. al	Advances in Automobile Engineering	2017
Practical Contactless Attacks on Hitag2-based Immobilizer and RKE Systems	Liu et. al	Int. Conf. on Computer, Communication and Network Technology	2018
Dismantling the AUT64 Automotive Cipher	Hicks et. al	IACR Transactions on Cryptographic Hardware and Embedded Systems	2018
Secure Free-Floating Car Sharing for Offline Cars	Dmitrienko, A. e Plappert, C.	Conference on Data and Application Security and Privacy	2017

Fonte: O autor (2019)

3.2.5.2 *Backward Snowballing*

Na primeira iteração *backward snowballing*, foram incluídos 20 novos artigos. Os artigos estão listados no Quadro 4.

Quadro 5 - Trabalhos selecionados na primeira iteração de *backward snowballing* **(continua)**

Título	Autor(es)	Publicação	Ano
A New Remote Keyless Entry System Resistant to Power Analysis Attacks	A. Moradi and T. Kasper	Int. Conf. on Information, Communications and Signal Processing	2009

Quadro 6 - Trabalhos selecionados na primeira iteração de *backward snowballing* **(continua)**

Título	Autor(es)	Publicação	Ano
AES Security Protocol Implementation for Automobile Remote Keyless System	Ni et. al	IEEE 65th Vehicular Technology Conference	2007
Algebraic and Slide Attacks on KeeLoq	Courtois et. al	Int. Workshop on Fast Software Encryption	2007
Attacks on the KeeLoq Block Cipher and Authentication Systems	Bogdanov, A.	3rd Conference on RFID Security	2007
Breaking Hitag2 Revisited	Immler, V.	2nd Int. Conf. on Security, Privacy, and Applied Cryptography Engineering	2012
Breaking Hitag2 with Reconfigurable Hardware	Stembera, P. and Novotny, M	14th Euromicro Conf. on Digital System Design	2011
Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed	Kasper et. al	AFRICACRYPT 2009: 2nd Int. Conf. on Cryptology in Africa	2009
Cryptanalysis of KeeLoq with COPACOBANA	Novotny, M. and Kasper, T.	Workshop on Special Purpose Hardware for Attacking Cryptographic Systems	2009
Cryptanalysis of the KeeLoq block cipher	Bogdanov, A.	IACR Cryptology ePrint Archive	2007
Cube Cryptanalysis of Hitag2 Stream Cipher	Sun et. al	10th Int. Conf. on Cryptology and Network Security	2011
Digital Signature Transponder	Kitsos et. al	RFID Security: Techniques, Protocols and System-on-Chip Design	2008
KeeLoq and Side-Channel Analysis -Evolution of an Attack	Paar et. al	Workshop on Fault Diagnosis and Tolerance in Cryptography	2009
Physical Cryptanalysis of KeeLoq Code Hopping Applications	Eisenbarth et. al	IACR Cryptology ePrint Archive	2008
Practical Algebraic Attacks on the Hitag2 Stream Cipher	Courtois et. al	International Conference on Information Security	2009
Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems	Yang et. al	Int. Conf. on Fuzzy Systems and Knowledge Discovery	2012
Security Analysis of an Open Car Immobilizer Protocol Stack	Tillich, S. and Wójcik, M.	INTRUST: Int. Conf. on Trusted Systems	2012
Smart Keys for Cyber-Cars: Secure Smartphone-based NFC-enabled Car Immobilizer	Busold et. al	3rd ACM Conf. on Data and Application Security and Privacy	2013

Quadro 7 - Trabalhos selecionados na primeira iteração de *backward snowballing* **(conclusão)**

Título	Autor(es)	Publicação	Ano
HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive	Wei et. al	IEEE Access	2017
SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision	Symeonidis et. al	Euro. Symposium on Research in Computer Security	2017

Fonte: O autor (2019)

3.2.6 Segunda Iteração

Na segunda iteração são avaliados os artigos que foram selecionados na primeira iteração.

3.2.6.1 *Forward Snowballing*

Na segunda iteração de *forward snowballing*, foram incluídos 12 novos artigos. Os artigos estão listados no Quadro 5.

Quadro 8 - Trabalhos selecionados na segunda iteração de *forward snowballing* **(continua)**

Título	Autor(es)	Publicação	Ano
Cryptographic properties of nested functions and algebraic immunity of the Boolean function in Hitag2 stream cipher	Shan et al.	Cryptographic and Communications	2014
Design of intelligent locks based on the triple KeeLoq algorithm	Chen et al.	Advances in Mechanical Engineering	2016
Fingerprint Identification Keyless Entry System	Lian et al.	Int. Journal of Electrical and Computer Engineering	2008
AES encryption algorithm keyless entry system	Xiaona Lv and Liping Xu	Int. Conf. on Electronics, Communications and Networks	2012
HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack	Wei et al.	Recent Advances in Systems Safety and Security	2016
Identification Technology Research on AES for Automobile Keyless System	Liu, L. et al.	Int. Conf. on Computational Intelligence and Software Engineering	2010
Improvement in Automobile Security System Controlled by Personal Computer via RF Link	Saikia et al.	Int. Journal of Electronics, Communication & Soft Computing Science and Engineering	2012
Iterative Side-Channel Cube Attack on KeeLoq	Yunfei Ma et al.	Instrumentation & Measurement, Computer, Communication and Control	2016

Quadro 9 - Trabalhos selecionados na segunda iteração de *forward snowballing* **(conclusão)**

Título	Autor(es)	Publicação	Ano
Robustness of remote keyless entry systems to intentional electromagnetic interference	Van de Beek, S et al.	Int. Symposium on Electromagnetic Compatibility	2014
Security of Wireless Embedded Devices in the Real World	Kasper et al.	Information Security Solutions (ISSE) 2011 – Securing Electronic Business Processes	2011
Vulnerability of Remote Keyless-Entry Systems Against Pulsed Electromagnetic Interference and Possible Improvements	Van de Beek et al.	IEEE Transactions on Eletromagnetic Compatibility	2016

Fonte: O autor (2019)

3.2.7 Terceira Iteração

Na terceira iteração são avaliados os artigos selecionados na segunda iteração. Porém, tanto na iteração de *backward* quanto na de *forward* não foram selecionados novos artigos, então o processo é finalizado.

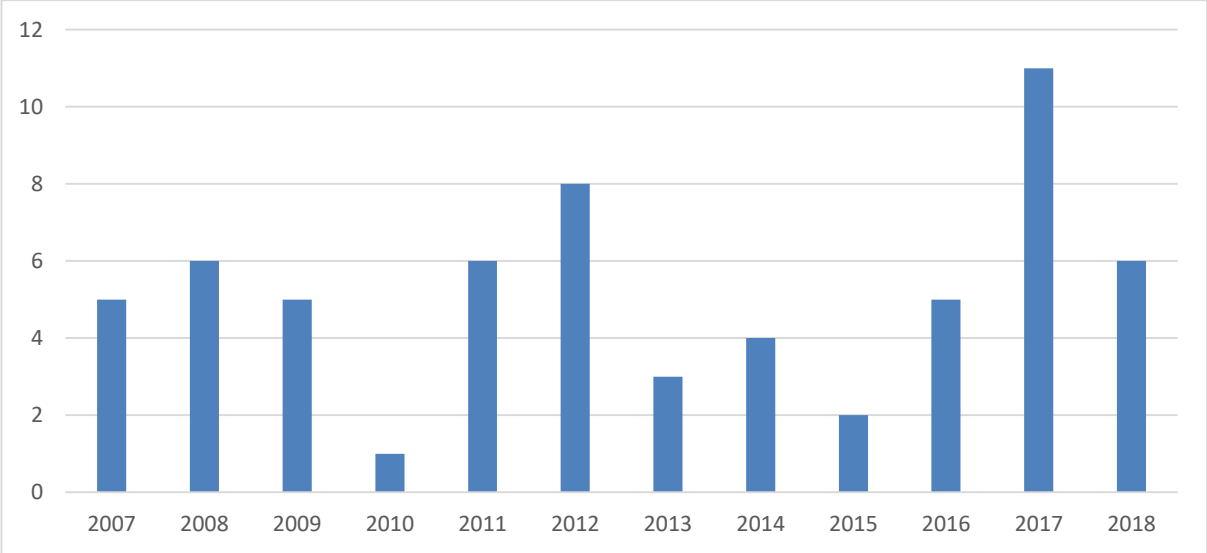
3.2.8 Resultados

O objetivo dessa seção é apresentar os resultados obtidos a partir dos 62 artigos selecionados na revisão sistemática realizada.

3.2.8.1 *Publicações por Ano*

A Figura 8 apresenta a quantidade de publicações por ano dos trabalhos selecionados. Vale ressaltar que os artigos pesquisados se limitam às publicações entre Janeiro de 2007 e Setembro de 2018.

Figura 8 - Quantidade de publicações x Ano

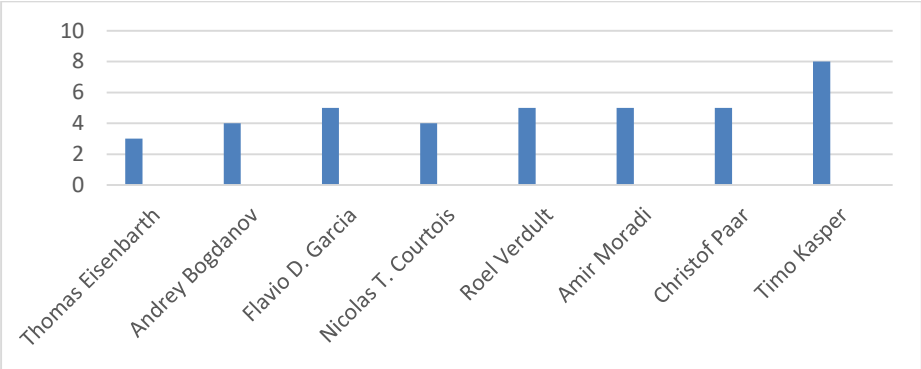


Fonte: O autor (2019)

3.2.8.2 *Principais Autores*

A Figura 9 apresenta os principais autores de acordo com a quantidade de publicações por autor. Como foram selecionados 62 artigos, só foram exibidos os autores com 3 ou mais publicações.

Figura 9 - Quantidade de publicações x Autores

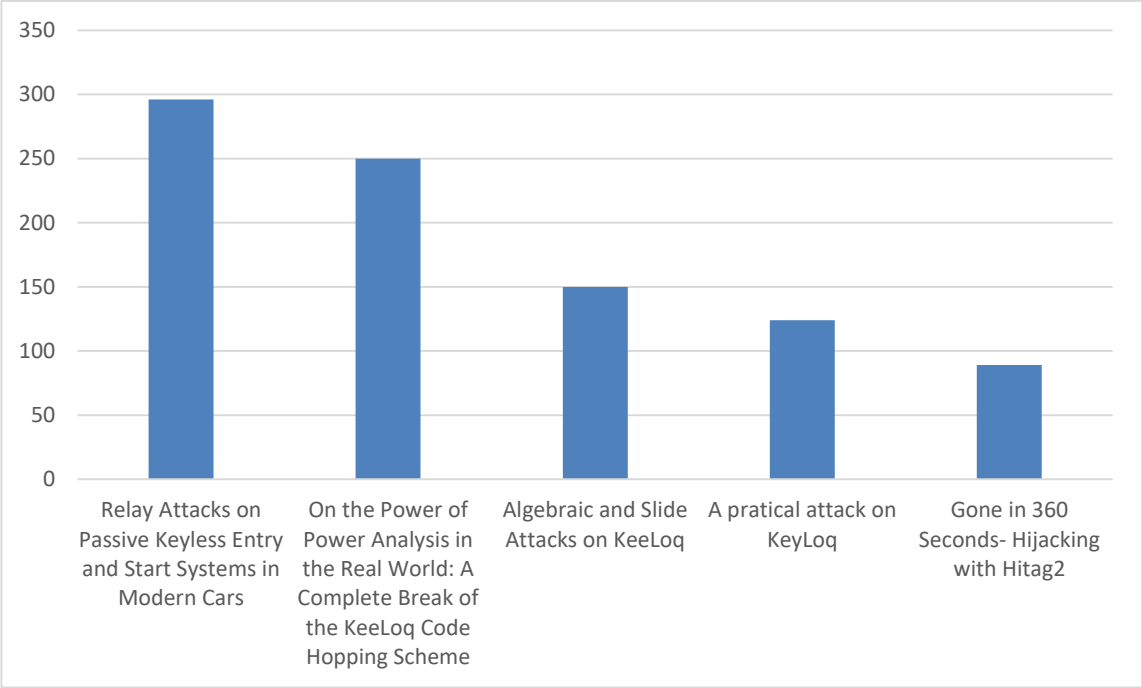


Fonte: O autor (2019)

3.2.8.3 *Artigos mais relevantes*

A Figura 10 apresenta os cinco artigos mais relevantes em relação ao número de citações no Google Scholar.

Figura 10 - Quantidade de referências no Google Scholar por publicação



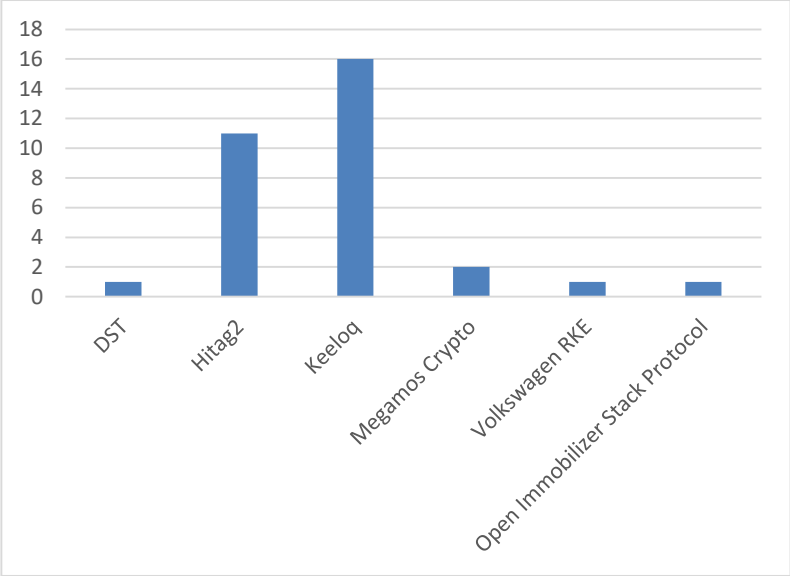
Fonte: O autor (2019)

3.2.8.4 *Principais Sistemas Estudados*

Dos artigos selecionados por essa revisão de literatura, 32 focam em sistemas utilizados pelo mercado. Entre esses sistemas estão: o Digital Signature Transponder (DST) da Texas Instruments, o Hitag2 da NXP/Philips, o Keeloq da Nanoteq, Megamos Crypto da Volkswagen/Thales, um sistema utilizado pelo grupo Volkswagen

e o Open Immobilizer Software Stack da Atmel. A figura a seguir (Figura 11) apresenta a quantidade de publicações por sistemas.

Figura 11 - Quantidade de publicações por sistemas



Fonte: O autor (2019)

3.3 REVISÃO SISTEMÁTICA DE PATENTES

O objetivo dessa Seção é explicar o procedimento realizado na Revisão Sistemática de Patentes desse trabalho.

3.3.1 Metodologia

Para realizar a revisão de patentes, foram utilizadas *strings* de buscas no Google Scholar. Essas *strings* foram elaboradas a partir das combinações das seguintes palavras-chave: "*keyless*", "*passive entry*", "*vehicle*", "*passive start*" e "*security*". Foram executadas buscas por patentes publicadas entre Janeiro de 2007 e Setembro de 2018 nos Estados Unidos.

A partir dos resultados obtidos foram excluídas as patentes que não estavam relacionadas a *Passive Keyless Entry and Start* (PKES). Essa exclusão baseou-se na leitura da patente.

3.3.2 Resultados

O objetivo dessa subseção é apresentar alguns dos resultados obtidos a partir das 161 patentes selecionadas na revisão sistemática realizada que estão disponíveis no apêndice dessa dissertação.

Entre as patentes encontradas, podemos destacar a patente de número US 9600948 B2 de Outubro de 2017 pertencente a Alps Electric Co Ltd. que trata-se de um PKES com um protocolo de comunicação entre veículo e a *key fob*, no qual existe pelo menos um modulador de sinal no veículo e um na *key fob* (MIYAZAWA, 2017).

O foco da patente está no funcionamento do protocolo, ele funciona com mudança de modulação que pode se dar através de mudança do modulador do sinal, da mudança nos métodos de modulação, ou da combinação de ambos. Através dessa técnica, a key fob estaria protegida contra *relay attack*, pois o atacante não tem informações sobre a modulação ou a mudança de modulador.

Já a patente de número US 14790223 B2 de Outubro de 2015 descreve uma PKES com uma *key fob* capaz de detectar *relay attack* (SEIBERTS; CHILDERS, 2015). Essa *key fob* é composta por um microcontrolador, um módulo para receber o sinal de despertar e um acelerômetro. Através do RSSI do sinal recebido e dos dados do acelerômetro, o microcontrolador é capaz de detectar *relay attack*. Nessa patente, o microcontrolador mantém a *key fob* em modo de espera caso o acelerômetro não detecte movimentos e caso o RSSI medido esteja abaixo de um limiar, evitando assim o *relay attack*.

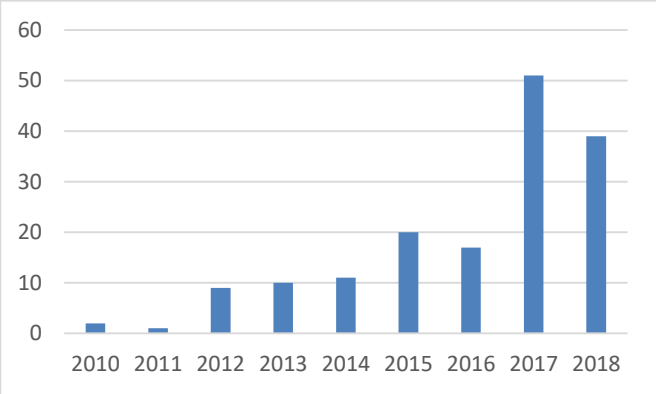
Na patente de número US 9045102 B2 de Junho de 2015 pertencente a TRW Automotive Italia SRL descreve um sistema de PKES com um conjunto de antenas para abertura remota e acionamento remoto da ignição do automóvel que utiliza o BLE como protocolo de comunicação (CARATTO; PIAZANNO; GINEVRO, 2015). A patente descreve um sistema com ao menos duas antenas que estão dispostas na parte frontal do veículo e próximas a uma ECU de modo que a fiação seja reduzida e simples que os demais sistemas do mercado. Além disso, existe uma antena auxiliar de baixa frequência cujo alcance auxilia a determinar o desejo de abertura do veículo. Porém, essa última antena é opcional.

A patente de número US 9963109 B2 de Maio de 2018 da Huf North America Automotive Parts Manufacturing Corp descreve um PKES composto por uma pluralidade de antenas e uma *key fob* para evitar o *relay attack* (LUO; NANTZ, 2018). Para tal, a *key fob* recebe os sinais das antenas e junto com constantes salvas em memória calcula se os ângulos dos vetores oriundos do campo eletromagnético formado pelos sinais das antenas estão corretos, caso os cálculos estejam incorretos, o sistema trata como um *relay attack*.

3.3.2.1 *Publicações por Ano*

A Figura 12 apresenta a quantidade de publicações por ano das patentes. Vale ressaltar que as patentes pesquisadas se limitam às publicações entre Janeiro de 2007 e Setembro de 2018.

Figura 12 - Publicações de patentes por ano

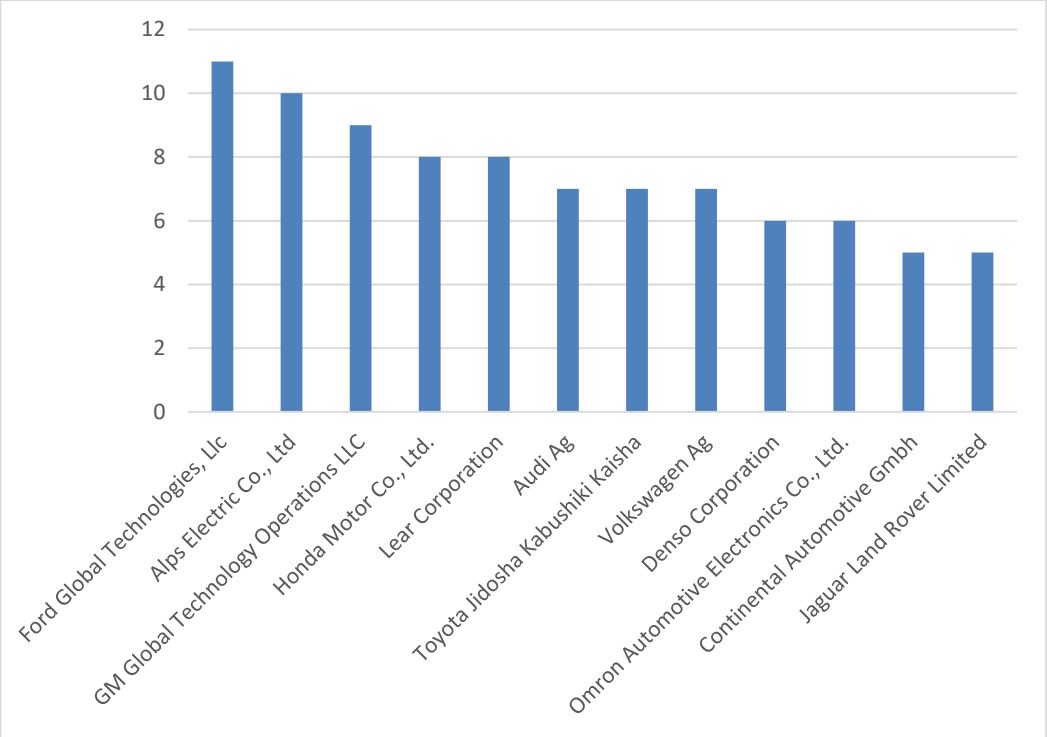


Fonte: O autor (2019)

3.3.2.2 *Publicações por Proprietários*

A Figura 13 apresenta a quantidade de publicações de patentes por empresas proprietárias das patentes. Nessa figura, estão apenas doze empresas com mais publicações de patentes.

Figura 13 - Publicações de patentes por proprietário



Fonte: O autor (2019)

3.4 REVISÃO EXPLORATÓRIA

Para aumentar a abrangência da pesquisa desse trabalho e para que conteúdos provenientes da indústria fossem incluídos no trabalho, uma revisão exploratória foi realizada.

Em revisões exploratórias não existe um processo bem definido a ser executado (POLLITT, 2007). Por isso, essas revisões podem ser consideradas tendenciosas, pois não podem ser replicadas. Nesse tipo de revisão, diversas fontes relacionadas ao tema são incluídas independentemente dos locais onde são publicadas e dos formatos que foram publicadas.

No caso da revisão exploratória realizada, o objetivo principal foi o de analisar sistemas comerciais encontrados nos mais diversos veículos de comunicação. Entre esses veículos podemos citar: sites de fabricantes, blogs e *datasheets* dos sistemas publicados pelos fabricantes.

3.4.1 Metodologia

De acordo com Pollitt (2007), não há um processo bem definido para se realizar uma revisão exploratória. Normalmente, há uma seleção de fontes e separação do conteúdo a partir de métodos mais bem definidos.

Na revisão exploratória deste trabalho, foram realizadas buscas por palavras-chave diretamente feitas no Google. As palavras-chave utilizadas foram: "*passive*", "*keyless entry*", "*vehicle*", "PKES" e "PEPS".

Além disso, foram realizadas buscas nos sites dos fabricantes de componentes veiculares encontrados pela revisão sistemática com o objetivo de mais informações sobre os sistemas desenvolvidos por essas empresas.

Diante dos resultados encontrados, o material foi lido e avaliada a relevância e aderência ao tema da pesquisa. Após a avaliação, o material encontrado foi discutido entre os pesquisadores da revisão sistemática e decidida a inclusão ou exclusão do conteúdo.

3.4.2 Resultados

Através da revisão exploratória foram encontrados dois modelos de PKES. Entre eles está o "*Perfectly Keyless*" da Bosch e um modelo conceitual (não existe comercialização dele) da Continental (CONTINENTAL, [s.d.]).

Dos modelos encontrados, tanto o modelo conceitual, quanto o comercial são sistemas que utilizam o Bluetooth Low Energy como tecnologia sem fio para PKES através do uso de smartphones. Esses resultados serão discutidos no próximo capítulo onde será feita uma análise de cada PKES.

3.5 CONSOLIDAÇÃO DAS REVISÕES

As Seções anteriores apresentaram os resultados encontrados nas revisões. Na Revisão Sistemática foram selecionados 6 sistemas de entrada e/ou partida: DST, Keeloq, Hitag2, Megamos Crypto, Open Immobilizer Software Stack da Atmel e o RKE

desenvolvido pelo Grupo Volkswagen. Já na Revisão exploratória (Seção 3.4), foram selecionados o Perfectly Keyless da Bosch e o modelo conceitual da Continental. Essas duas revisões totalizaram 8 sistemas, o Quadro 6 sumariza esse resultado.

Quadro 10 - Sistemas selecionados por revisão

	Revisão Sistemática	Revisão Exploratória
DST	X	
Keeloq	X	
Hitag2	X	
Megamos Crypto	X	
Volkswagen Group RKE	X	
Megamos Crypto	X	
Open Immobilizer Software Stack	X	
Perfectly Keyless - Bosch		X
Continental Keyless		X

Fonte: O autor (2019)

Esses sistemas foram selecionados devido à importância deles no mercado. Para se ter uma noção dessa importância, o DST chegou a ser utilizado em mais de 150 milhões de veículos (BONO et al., 2005). Já o Keeloq foi adotado por diversos fabricantes como, por exemplo, GM, Volkswagen Group, Volvo, Toyta, Honda, Fiat, entre outros[16]. O Hitag2 é utilizado por 34 montadoras de veículos em mais de 200 modelos (VERDULT; GARCIA; BALASCH, 2012). O Megamos Crypto, segundo o fabricante, produziu mais de 100 milhões dispositivos (VERDULT; GARCIA; EGE, 2015). O RKE do Grupo Volkswagen, que é um dos líderes mundiais em vendas, foi utilizado em modelos como: Fox, Golf, Audi A1, Audi Q3, entre outros (GARCIA et al., 2016).

Através dos resultados encontrados nas duas revisões, evidenciou-se a importância dos PKES na indústria automobilística pela presença de grandes fabricantes, como a Bosch, Philips e Continental e pela quantidade de veículos afetados.

A próxima seção visa analisar diversos aspectos dos sistemas selecionados, embora nem todas as características se aplicam a todos os sistemas e/ou não foram

[16] https://en.wikipedia.org/wiki/KeeLoq

encontradas informações suficientes para analisar determinada característica do sistema, por se tratar de um sistema de uso comercial.

3.6 PRINCIPAIS REQUISITOS ANALISADOS

Diante dos diversos requisitos que podem ser analisados em um sistema de PKES, entre eles usabilidade, tipo de rede, tamanho da chave de criptografia, autenticação, consumo de bateria, algoritmo de criptografia e custo, essa pesquisa limitou-se a focar em aspectos de segurança. As subseções a seguir analisam o tipo de rede utilizada, o tamanho da chave, o protocolo de autenticação, criptografia, vulnerabilidades e ataques para cada sistema.

3.6.1 Dispositivos

Uma das principais decisões a serem tomadas em um projeto de um sistema de PKES e RKE é quais dispositivos serão utilizados. A escolha do dispositivo impacta diretamente em outros aspectos como usabilidade, custo, capacidade de processamento, etc.

Em diversos sistemas de entrada e partida, o uso da *key fob* (Figura 14) tem sido bastante utilizada, como é o caso, por exemplo, do DST, Hitag2, Keeloq, Volkswagen Group RKE e Megamos Crypto. Já outros estudos na literatura apontam para o uso de impressões digitais para controle de acessso ao veículo, como é o caso de (CHIH-NENG; HUANG-BIN; BO-CHIUAN, 2008). Porém, em sistemas mais modernos, como do Perfectley Keyless da Bosch e o modelo da Continental, o uso de celulares e *wearables* tem se mostrado uma tendência, como inclusive, já tem sido veiculado na mídia a adoção dos celulares por grandes montadoras (CNET, 2018).

Figura 14 - Key fob com Hitag2

Fonte: Verdult, Garcia e Balasch (2012)

3.6.2 Rede

Um dos principais requisitos a ser analisado em um PKES é que tipo de rede o sistema utiliza. O tipo de rede selecionada influencia, por exemplo, na distância em

que o veículo pode ser aberto, o quão fácil o sinal penetra em obstáculos e com que velocidade os dados podem trafegar na rede formada entre o carro e a chave. Além disso, a escolha da rede também afeta a segurança, pois cada tipo de rede apresenta suas limitações e falhas de segurança. Uma rede sem fio de longo alcance, por exemplo, permite também que o atacante esteja distante.

Nos sistemas mais antigos, como o Hitag2, DST, Keeloq, Megamos Crypto, Volkswagen RKE e nos sistemas da Atmel que fazem uso do Open Immobilizer Software Stack, é muito comum o uso RFID (Radio Frequency IDentification) que possuem sinais LF (do inglês, *low frequency*) de até 125 kHz para imobilizadores e de sinais UHF (do inglês, *ultra high frequency)* de até 433 MHz para RKE. No caso dos imobilizadores, uma vez que o motorista se encontra dentro do veículo, não há necessidade de um grande alcance da rede. Já no caso dos RKE, poucos metros são suficientes para apertar o botão e abrir uma porta ou se aproximar para destravá-lo no caso dos PKES.

Já os sistemas mais novos, encontrados na revisão exploratória, utilizam a tecnologia *bluetooth low energy* (BLE), que opera a uma frequência de 2.4-2.5 GHz. Essa frequência de rede, além de permitir distâncias de aproximadamente 50 metros, também permitem trafegar dados em uma velocidade de até 1Mbit/s. Esse ganho em transmissão de dados possibilita, por exemplo, o uso de uma chave de criptografia maior que aumenta a segurança dos sistemas.

O Quadro 7 resume as redes estudadas nos sistemas analisados.

Quadro 11 - PKES e as redes utilizadas

Sistema	Rede	Frequência	Distância
DST	LF	134,2 kHz – 123,2 kHz	< 50cm
Keeloq	UHF	433MHz	Poucos metros
Hitag2	LF/UHF	125 khz (imobilizador)/ 433 MHz (RKE)	< 50 cm/ Poucos metros
Megamos Crypto	LF	100-150 kHz	< 50 cm
Volkswagen RKE	UHF	433,92 MHz – 434,4 MHz	Poucos metros
Atmel	LF	125 kHz	< 50cm
Continental	BLE	2,4-2,5 GHz	≅ 50 m
Bosch	BLE	2,4-2,5 GHz	≅ 50 m

Fonte: O autor (2019)

3.6.3 Tamanho da chave de criptografia

Um outro fator importante na segurança dos sistemas de entrada e partida é o tamanho da chave. Obviamente, o simples aumento do tamanho da chave nem sempre é o suficiente para garantir a segurança de um PKES. Além disso, o aumento da chave significa um aumento considerável no processamento necessário para realizar a criptografia dos dados e um aumento na velocidade necessária da rede para trafegar dados, caso contrário, o usuário perceberá o atraso entre a ação de apertar um botão para abrir o carro e o tempo necessário para autenticar ou o usuário poderá se aproximar do veículo e tentar abrir a porta antes do veículo destravar automaticamente em um PKES.

Nos sistemas analisados os tamanhos da chave variam bastante, o Quadro 8 apresenta os valores encontrados. Novamente não foram encontradas informações nos sistemas da Bosch e da Continental.

Quadro 12 - Chaves utilizadas

Sistema	Tamanho da chave
DST	40 bits
Hitag2	64 bits
Keeloq	48 bits
Megamos Crypto	96 bits
Open Immobilizer Software Stack	128 bits
Volkswagen RKE	Até 128 bits

Fonte: O autor (2019)

3.6.4 Autenticação

Um dos fatores mais importantes em um sistema de segurança é a autenticação.

Os sistemas analisados em uma classificação mais ampla se dividem em duas: autenticação mútua (bilateral), onde o carro realiza a autenticação da chave e vice-versa, e a autenticação unidirecional, onde apenas um lado realiza autenticação. Como em boa parte dos sistemas analisados a chave possui um processamento limitado, fica para o carro a tarefa de autenticação no caso de uma autenticação unidirecional.

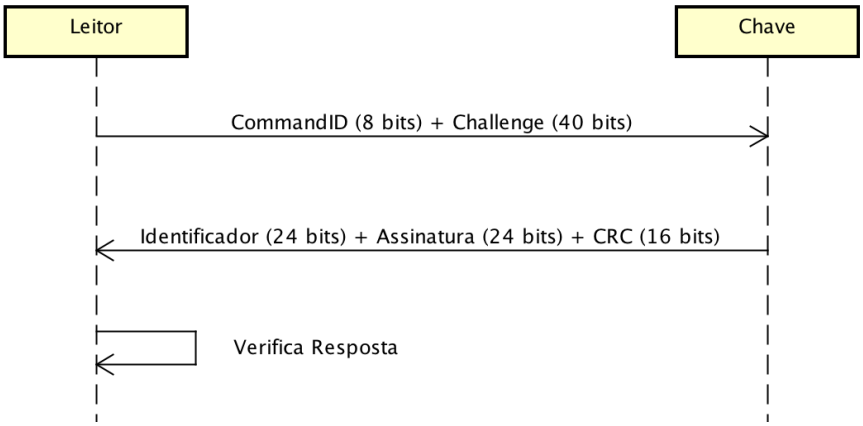
Nas seções seguintes serão analisadas, com mais detalhes, as autenticações do DST, Hitag2, Keeloq, Megamos Crypto, Open Immobilizer Software Stack e dos RKE utilizados em veículos do grupo Volkswagen. Infelizmente, não foram

encontradas informações sobre a autenticação usada nos sistemas da Bosch e da Continental.

3.6.4.1 *DST*

O DST (Digital Signature Transponder) utiliza um protocolo de autenticação conhecido como *challenge-response* (BONO et al., 2005), onde o leitor (carro) começa enviando um desafio ao *transponder* (chave), esse comando possui 8 bits para identificar a operação de autenticação e 40 bits do desafio (Figura 15). O *transponder* criptografa o desafio com os 40 bits da chave compartilhada com o leitor, onde os 24 bits menos significativos fazem parte de uma assinatura. O *transponder* responde ao desafio com 24 bits do identificador, 24 bits da assinatura e 16 bits de CRC (Cyclic Redundancy Check). Na primeira transmissão, os 16 bits de CRC são secretos, mas o fabricante usou o mesmo valor para todos dispositivos. A partir da chave compartilhada e dos 16 bits secretos de CRC, o leitor consegue verificar se a assinatura do *transponder* é correta.

Figura 15 - Autenticação do DST



Fonte: O autor (2019)

3.6.4.2 *Hitag2*

O Hitag2 se utiliza de *challenge-response* com autenticação mútua entre o carro (*reader*) e a chave (*transponder*), ou seja, carro e chave verificam a autenticidade um do outro. A seguir o passo a passo realizado na autenticação do Hitag2 (ŠTEMBERA; NOVOTNÝ, 2011):

- O carro (*reader*) envia comando de *authentication* (11000) para a chave (transponder)
- O *transponder* responde com o (11111) seguido do identificador.
  (daqui em diante a comunicação ocorre criptografada)

- O carro envia 32 bits do autenticador criptografado e 32 bits de um número pseudoaleatório gerado
- O *transponder* criptografa a chave compartilhada que possui com o número pseudoaleatório recebido e se o valor recebido corresponder ao valor gerado, ele responde com a resposta ao desafio.

3.6.4.3 *Keeloq*

O processo de autenticação do Keeloq acontece de maneira unidirecional e implícita. Existem duas possibilidades de autenticação no Keeloq, uma delas faz uso de um algoritmo chamado de *rolling code* ou *hopping code* e a outra é conhecida como IFF (do inglês, *Identifie Friend or Foe*) (INDESTEEGE et al., 2008).

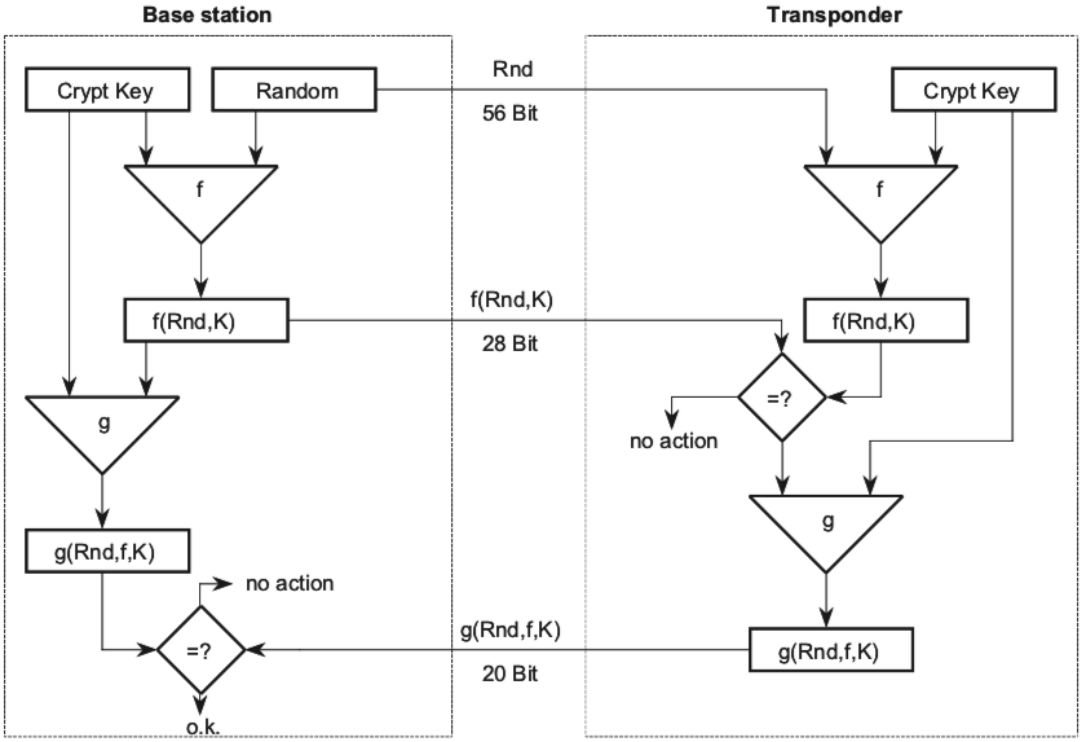
No modo de autenticação conhecido como *hopping code,* o carro e a chave possuem um contador sincronizado entre eles que varia de 16 a 18 bits. Ao pressionar o botão, a chave criptografa um código de 32 bits a partir de um *discrimination value*, um contador e 4 bits do comando (abrir, fechar, etc.) e envia ao receptor. Essa criptografia é realizada a partir da chave compartilhada. Quando o receptor recebe o comando, ele decodifica com sua chave compartilhada e verifica se o discrimination value é o mesmo que ele possui e se o contador está dentro da janela permitida. Caso positivo, o comando é executado (PAAR et al., 2009).

Já na autenticação IFF, a autenticação é realizada quando o veículo envia um desafio de 32 bits a chave que, por sua vez, criptografa o desafio com a chave compartilhada e responde ao carro. Ao receber a resposta ao desafio, o carro descriptografa a resposta e verifica se ela corresponde (INDESTEEGE et al., 2008). Como nesse tipo de autenticação não há intervenção do usuário, ele pode ser usado em imobilizadores.

3.6.4.4 *Megamos Crypto*

No Megamos Crypto a autenticação é mútua, ou seja, carro e chave autenticam um ao outro. O processo de autenticação tem início com o carro lendo o identificador da chave. Em seguida, o veículo envia um número aleatório de 56 bits para a chave. Então, ambos criptografam o número randômico gerado pelo carro com a chave compartilhada. Depois, o carro envia o resultado da criptografia para a chave que compara os resultados. Caso positivo, a chave criptografa o resultado com sua chave e envia ao carro, que confirma a autenticidade da chave a partir da mesma operação realizada pelo carro. A (Figura 16) ilustra o processo de autenticação.

Figura 16 - Autenticação mútua do Megamos Crypto



Fonte: Verdult, Garcia e Ege (2015)

3.6.4.5 *Volkswagen Group RKE*

Os RKE que foram analisados em Garcia et al. (2016) se utilizam de uma autenticação implícita. Nesses sistemas, a autenticação é unidirecional com o carro autenticando a chave. Cada comando enviado do *key fob* para o carro é decodificado e nele há um contador que é incrementado cada vez que um comando é enviado. Ao receber um comando, o carro verifica se o contador está dentro de uma janela válida e, caso esteja, executa o comando recebido. Para que esse tipo de autenticação funcione corretamente, tanto carro como chave devem ser sincronizados.

3.6.4.6 *Open Immobilizer Software Stack*

Na especificação desenvolvida pela Atmel, a autenticação pode ser configurada como mútua (bilateral) ou unilateral (ATMEL, 2012). A Figura 17 ilustra a autenticação mútua, onde o carro e a chave compartilham duas chaves AES. Inicialmente, o carro faz um *request* para leitura do ID da chave (comando ReadUID). Ao receber a resposta da chave, o carro verifica se a chave está pareada. Caso positivo, o carro inicia o processo de autenticação (comando Start Authentication).

O processo de autenticação, propriamente dito, inicia-se com o carro gerando um desafio (*challenge*) a partir de um numero randômico gerado (RandN) criptografado com a chave AES 1. Desse resultado, o carro extrai RandM (número randômico gerado a partir de RandN) bits para ser enviado à chave junto com o Rand

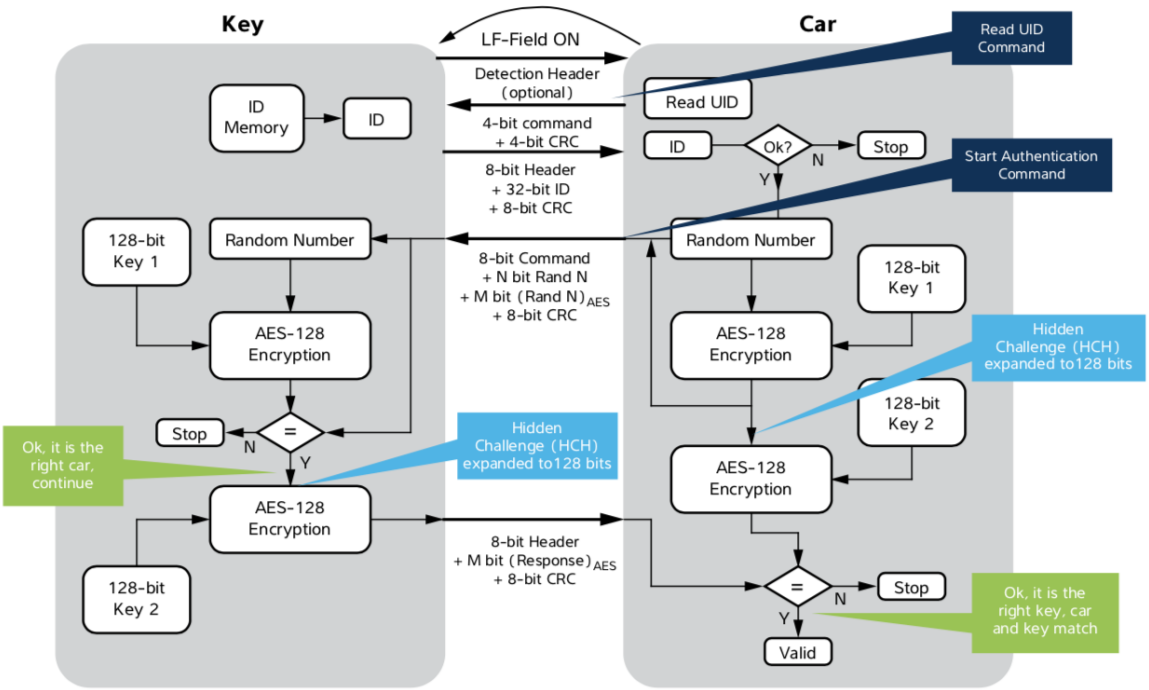
N. A chave então verifica a autenticidade a partir de RandN e RandM e a sua chave compartilhada e, em caso de sucesso, o carro está autenticado na chave. Para fazer a autenticação mútua, a chave utiliza o primeiro resultado da autenticação como entrada para a segundo passo da criptografia com a outra chave AES compartilhada e seleciona M bits, e envia ao carro, que por sua vez usa sua chave para verifica a autenticidade da resposta para efetuar a autenticação da chave finalizando assim a autenticação mútua.

Nota-se que a autenticação mútua utilizada no Open Immobilizer Software Stack se assemelha bastante com a realizada pelo Megamos Crypto descrita na Seção 3.5.4.4. Porém, a autenticação utilizada pela Atmel faz uso de duas chaves compartilhadas, o que torna o sistema mais seguro.

Entre os sistemas analisados, nota-se que em sistemas mais modernos como, por exemplo, o Megamos Crypto e o Open Immobilizer Software Stack da Atmel o processo de autenticação utilizado é mútuo entre veículo e chave. Além disso, percebe-se o uso de janelas de sincronização ou contadores para evitar *replay attack* como é o caso do Keeloq e do Megamos Crypto (EISENBARTH et al., 2008; VERDULT; GARCIA, 2015), porém esse tipo de proteção não é o suficiente contra *relay attacks.*

O Quadro 9 resume o tipo de autenticação utilizada pelos sistemas avaliados, para o sistema da Bosch e da Continental não foram encontradas informações.

Figura 17 - Autenticação mútua do Open Immobilizer Software Stack da Atmel



Fonte: Atmel (2012)

Quadro 13 - Sistemas e tipos de autenticação

Sistema	Autenticação
DST	unilateral
Hitag2	unilateral
Keeloq	unilateral
Megamos Crypto	mútua
Open Immobilizer Software Stack	mútua
Volkswagen RKE	unilateral

Fonte: O autor (2019)

3.6.5 Criptografia

Junto com a chave e o protocolo de autenticação, a criptografia utilizada em um sistema de PKES é um dos fatores mais importantes no que tange a questão da segurança. Porém, muitos dos RKE e imobilizadores desenvolvidos pela indústria automobilística foram criados baseados na confidencialidade do algoritmo e do protocolo utilizado. Essa confidencialidade contraria o principio de Kerkchoff que diz: “Um sistema criptográfico deve ser seguro mesmo se tudo, exceto a chave, seja de domínio público”.

O uso de algoritmos de criptografia já conhecidos pela comunidade acadêmica aumenta a confiabilidade do algoritmo em questão, já que ele foi testado e estudado pela comunidade científica, em vez de uma pequena equipe de engenheiros. Entre os sistemas analisados, apenas o Open Immobilizer Software Stack da Atmel sugere o uso de um algoritmo padrão, que no caso é o AES (do inglês, *Advanced Encryption Standard*) (TILLICH; WÓJCIK, 2012). Os demais sistemas optaram pelo uso de algoritmos proprietários baseados em algoritmos abertos, foram eles: cifra de Feistel não balanceada, usado pelo DST (BONO et al., 2005), NLFSR (do inglês, *non linear feedback shift register*) usado pelo Keeloq (PAAR et al., 2009), uma combinação do NLFSR com uma GLFSR (do inglês, *galois linear feedback shift register*), usado no Megamos Crypto (WANG; YU, 2005a), uma LFSR (do inglês, *linear feedback shift register*) e uma função não-linear, usadas no Hitag2 (ŠTEMBERA; NOVOTNÝ, 2011) e o AUT64 e XTEA, usados pela Volkswagen (GARCIA et al., 2016). Nos sistemas da Bosch e da Continental não foram encontradas informações sobre que algoritmo é utilizado.

3.6.5.1 *DST*

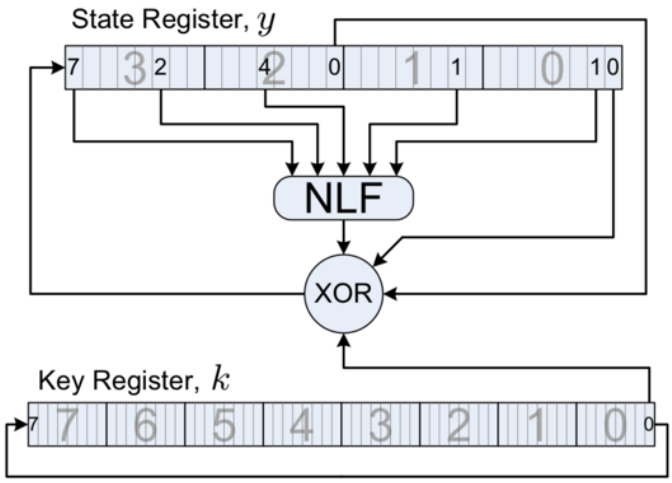
No DST o algoritmo de criptografia utilizado é proprietário e baseado em uma cifra de Feistel desbalanceada. Nesse algoritmo, o leitor usa uma chave de 40 bits para criptografar o desafio e enviar uma resposta truncada de 24 bits. O receptor que possui a mesma chave de criptografia compara o resultado do leitor com a resposta esperada (BONO et al., 2005).

3.6.5.2 *Keeloq*

O Keeloq usa um algoritmo proprietário composto por uma chave de 64 bits e codificação em blocos de 32 bits através de uma NLSFR (do inglês, *non-linear feedback shift register*), onde o *feedback* depende linearmente de 2 bits de registro, sendo eles 1 bit da chave e 1 bit da função não-linear (EISENBARTH et al., 2008).

Na inicialização do algoritmo, a chave e o estado devem ser armazenadas nos seus respectivos registradores, como mostra a Figura 18. Então, a cada ciclo de clock, o registrador da chave é deslocado para a direita, assim como o registrador do estado. Após 528 ciclos de *clock*, o registrador do estado conterá o texto cifrado.

Figura 18 - Cifrador do Keeloq



Fonte: Paar et al. (2009)

3.6.5.3 *Hitag2*

O Hitag2 usa um algoritmo proprietário de codificação em fluxo com uma chave de 48 bits (VERDULT; GARCIA; BALASCH, 2012). Esse algoritmo se utiliza de uma LFSR (do inglês, *Linear Feedback Shift Register*) e uma função não-linear para saída da *keystream*. Em 2007, após ter sido descoberto por engenharia reversa (COURTOIS; O'NEIL; QUISQUATER, 2009), o Hitag2 chamou atenção da comunidade científica e teve diversos trabalhos publicados a respeito (BENADJILA et al., 2017).

3.6.5.4 *Megamos Crypto*

A criptografia realizada pelo Megamos Crypto consiste em: uma função GLFSR (do inglês, *Galois Linear Feedback Shift Register*), uma NFSR (do inglês, *non-linear Feedback Shift Register*), e três registradores de 7 bits cada (VERDULT; GARCIA; EGE, 2015).

3.6.5.5 *Volkswagen Group RKE*

Os veículos fabricados e equipados com o RKE do Grupo Volkswagen até 2005 não faziam uso de algoritmos de criptografia e apenas utilizam uma ofuscação de código. Já os modelos fabricados a partir de 2004, alguns modelos passaram a ser equipados com cifradores AUT64 (um cifrador iterativo que utiliza 8 blocos de 8 *bytes* cada) ou XTEA (um cifrador de blocos baseados em uma Feistel com blocos de 64 bits e chaves de 128 bits) (GARCIA et al., 2016).

3.6.5.6 *Atmel Open Immobilizer Software Stack*

O protocolo criado pela Atmel não possui um algoritmo definido. Ele especifica um modúlo de criptografia e recomendam que seja utilizado algum algoritmo publicamente conhecido e testado. Nos *datasheets* dos produtos fabricados pela Atmel eles utilizam o AES (do inglês, *Advanced Encryption Standard*) com uma chave de 128 bits (ATMEL, 2012).

O Quadro 10 resume os algoritmos utilizados pelos sistemas pesquisados na Seção 3.5.5.

Quadro 14 - Algoritmos de criptografia utilizados

Sistema	**Algoritmo**
DST	Cifra de Feistel não balenceada
Hitag2	LFSR + função não-linear
Keeloq	NLFSR
Megamos Crypto	NLFSR + GLFSR
Open Immobilizer Software Stack	AES
Volkswagen RKE	AUT64 ou XTEA

Fonte: O autor (2019)

3.7 VULNERABILIDADES

Essa seção tem como objetivo elencar as vulnerabilidades encontradas nos sistemas encontrados na revisão da literatura. Os sistemas encontrados pela revisão exploratória só possuem informações disponibilizadas pelos fabricantes, logo não

serão abordados nessa seção. As subseções a seguir apresentam as vulnerabilidades de cada sistema.

3.7.1 DST

Uma das principais fraquezas do DST é o tamanho da chave. Com apenas 40 bits, é possível fazer uma busca exaustiva para encontrar a chave utilizada (BONO et al., 2005).

3.7.2 Hitag2

A principal vulnerabilidade do Hitag2 é devida à criptografia fraca e a chave de 48 bits. De acordo com Verdult, Garcia e Balasch (2012), um outro problema é devido à dependência entre sessões, o que faz com que 16 bits se repitam durante a troca de mensagens entre carro e chave. Além disso, com uma probabilidade de 25%, os bits do cifrador são determinados por apenas 34 bits do estado interno. Como consequência, uma em cada quatro tentativas de autenticação revela um bit de informação da chave secreta.

Ainda de acordo com Verdult, Garcia e Balasch (2012), um outro problema encontrado no Hitag2 é que não há também um gerador de números pseudo-aleatórios. Além disso, o *transponder* responde com dados conhecidos quando é executado um comando de leitura no bloco de memória onde a identificação do *transponder* é armazenada. Outra vulnerabilidade é que os 48 bits do estado interno do cifrador só são gerados por blocos de 32 bits e os outros 16 bits são persistidos por sessões diferentes (a chave deveria ser gerada de uma única vez).

3.7.3 Keeloq

Uma das vulnerabilidades do Keeloq é sua chave de apenas 64 bits, além disso, ele implementa o protocolo de *challenge-response* onde os "*challenges*" não são autenticados, fazendo com que um atacante possa obter conjuntos de texto não cifrado e texto cifrado diretamente do controle remoto (INDESTEEGE et al., 2008).

Estudos também confirmaram que os fabricantes também utilizam a mesma chave-mestre na maioria dos seus produtos (SHEETRIT; WOOL, 2011). Caso isso ocorra, é possível recuperar a chave usando *side channel attack* no receptor.

3.7.4 Megamos Crypto

De acordo com Verdult, Garcia e Ege (2015) as principais vulnerabilidades do Megamos Crypto são:

- A ausência de um gerador de números pseudoaleatórios;
- Os últimos passos do protocolo de autenticação firnecem ao atacante 15 bits em texto não cifrado;

- O estado interno da cifra é de 56 bits, diferentemente da chave que é de 96 bits;
- Em muitos *transponders* vários bits em sequencia são zeros na chave;
- A chave é criada em operações de escrita de blocos de 16 bits, ou seja, não é de maneira atômica;
- Função que gera o próximo estado pode ser invertida;
- A memória é bloqueada/desbloqueada através de um *pin code* padrão conhecido.

3.7.5 Volkswagen RKE

De acordo com Garcia et al. (2016), a versão do RKE utilizada até 2005 em alguns veículos do grupo Volkwagen só utilizavam uma função de ofuscação de código, sendo muito fácil quebra-la. Já, os veículos fabricados entre 2005 e 2016 possuem como fraqueza o uso de uma chave global fixa na *key fob*, fazendo com que a autenticação entre os modelos mude apenas no identificador e o contador.

3.7.6 Atmel Open Immobilizer Software Stack

De acordo com Tillich e Wójcik (2012), as vulnerabilidades no Open Immobilizer Software Stack são: os comandos “ReadUID” e “Write Memory Access Protection” ocorrem de maneira não autenticada. Já no comando “LearnSecretKey” não é verificaca a integridade. Além disso, a chave não gera um número pseudoaleatório e não existe um *timestamp* ou identificador entre seções.

3.8 ATAQUES

Diante das vulnerabilidades expostas na seção anterior, essa seção visa analisar os ataques existentes na literatura para os sistemas pesquisados. As subseções a seguir apresentam cada um desses ataques para cada sistema.

3.8.1 DST

Devido ao tamanho da chave, apenas 40 bits, um possível ataque ao DST (BONO et al., 2005) é atraves da busca exaustiva (força bruta). A partir de dois pares *challenge-reponse*, é possível descobrir a chave em menos de uma hora. Além disso, também mostrou-se possível através de *time-memory tradeoff* executar o ataque em poucos minutos (BONO et al., 2005).

3.8.2 Hitag2

Após ter o algoritmo descoberto por engenharia reversa em 2007 (VERDULT; GARCIA; BALASCH, 2012), o Hitag2 passou a ser alvo da comunidade científica de criptografia e diversos ataques surgiram, entre eles podemos citar:

- *Algebric Attack*: Esse ataque consiste em transformar o estado do cifrador em um sistema de equações e utilizar algoritmos de satafistabilidade booleana para resolver o sistema e recuperar a chave. No ataque realizado em Courtois, O'Neil e Quisquater (2009) é necessário escutar quatro sinais e leva cerca de 2 dias para resolvê-lo. Depois Soos, Nohl e Castelluccia (2009) fez uma melhoria no ataque e reduziu o tempo para 8 horas.
- *Brute force attack* (ŠTEMBERA; NOVOTNÝ, 2011): Esse ataque utiliza busca exaustiva da chave a partir de dois pares de *challenges-responses* e, no pior caso, leva cerca de 103 minutos. O ataque usa um *cluster* COPACOBANA (do inglês, *Cost-Optimized Parallel Code-Breaker*) com 120 FPGAs (do inglês, *Field Programmable Gate Array*).
- *Criptoanalytic attack* por Sun et al. (2011): é um ataque que procura por relações lineares entre o cifrador e os bits de saída para reduzir o tamanho do cifrador e dimiuir o tempo de ataque. Com essa técnica o ataque é reduzido a menos de um minuto, porém esse ataque necessita que sejam escolhidos os vetores de inicialização do cifrador, o que não é possível em um ataque na prática.
- *Criptoanalytic attack* por Verdult, Garcia e Balasch (2012): Esse ataque faz uso da dependência de 25% entre bits do cifrador, com isso o atacante pode realizar 136 tentativas de autenticação a partir de um ID de transponder válido, com isso ele obtem 136/4 = 34 bits e os demais bits são obtidos por busca exaustiva. Esse ataque leva em torno de 6 minutos para ser executado.
- *Malleability attack*: Realizado por Verdult, Garcia e Balasch (2012), esse ataque consiste em escutar um comando de autenticação válido para uso futuro. A partir da autenticação válida escutada, um comando de autenticação com bits de redundância maior que o cifrador permita pode ser gerado. Então, como o cifrador não possui um *response* correto para o *challenge* para o comando de autenticação, ele responde com sucesso ao comando de autenticação. Então, é feita a busca exaustiva para achar o comando criptografado de leitura.
- *Time/memory tradeoff attack*: Realizado por Verdult, Garcia e Balasch (2012) esse ataque consiste em gerar tabelas pré-computadas e escutar

uma autenticação válida para obter a chave criptografada e a partir daí realizar buscas nas tabelas para encontrar a chave.

3.8.3 Keeloq

Assim como o Hitag2, o algoritmo do Keeloq se tornou público (BOGDANOV, 2007). Então, o sistema também tornou-se alvo de diversos estudos da comunidade de criptografia, tendo sido encontrado diversos tipos de ataques como: *Time-Memory Tradeoff, Slide Attack, Algebric Attack, Related Key* e combinações entre esses ataques (INDESTEEGE et al., 2008).

3.8.4 Megamos Crypto

De acordo com Verdult, Garcia e Ege (2015), o Megamos Crypto é suscetível a três ataques: *Time-memory trade-off, Partial key update attack* e *Weak Key Attack*.

O *Time-memory trade-off* é um ataque que requer um tempo muito grande para ser realizado no Megamos Crypto, sendo considerado muito dificil de ser colocado em prática. Para efetuar o ataque, é necessário interceptar duas autenticações com sucesso entre o carro e a chave, e em seguida, a partir de tabelas pré-computadas realizar buscas para encontrar a chave.

O *Partial key update attack* é um ataque que consiste em modificar a chave para bloquear o controle. No entanto, para efetuar esse ataque é preciso que o controle (chave) não tenha sido configurado com proteção à leitura. No ataque, é preciso escutar uma autenticação entre carro e chave, para então, explorar o fato da chave não desafiar o carro. Então, o atacante executa comando de escrita em um dos blocos 16 bits que contém a chave, para cada tentativa de escrita ele modifica o par do desafio da autenticação necessária para cada comando de escrita.

Já o *Weak key attack* consiste em explorar a baixa entropia da chave, onde vários bits da chave são zeros. Nesse ataque, o atacante pré-computa tabelas com possíveis chaves e escuta uma autenticação entre carro e chave. A partir daí, tendo conhecimento de um par *challenge-reponse* e das tabelas computadas, o atacante faz buscas exaustivas na tabela para descobrir o estado do cifrador e recuperar a chave.

3.8.5 Volkswagen RKE

De acordo com Garcia et al. (2016), os RKE utilizados em parte dos veículos do grupo Volkswagen são configurados a partir de poucas chaves criptografadas. De posse dessas chaves, o atacante pode simplesmente escutar comunicações entre carro e chave e a partir das chaves descobrir a chave secreta do controle. Além dessa falha, o sistema está sujeito a DoS (do inglês, *Denial of Service*), onde o atacante pode modificar o comando gerado pela chave alterando o contador, utilizado fazendo

com que o veículo não aceite comandos do controle original.

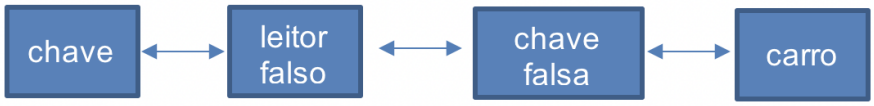
3.8.6 Atmel Open Immobilizer Software Stack

De acordo com Tillich e Wójcik (2012), o Open Immobilizer Software Stack da Atmel está sujeito aos seguintes ataques:

- *Relay Attack with Genuine Key Fob*

  Esse ataque consiste em usar um leitor falso e uma *key fob*, falsa como mostrado na Figura 19.

Figura 19 - Replay attack with Genuine Key Fob



Fonte: Adaptada de Tillich e Wójcik (2012)

- *Tracking*

  O ataque de Tracking se dá através de um comando não autenticado e que retorna um resultado previsível para o atacante e que o resultado é único por *key fob*, ou seja, o mesmo comando geraria um resultado diferente em outra *key fob*. O comando “ReadUID” é um comando que ocorre sem autenticação. Nesse caso, o tracking por si só não oferece riscos, mas provê informações ao atacante.

- *Denial-of-Service Attack*

  O comando “LearnSecretKey” usa a chave criptografada, mas não verifica a integridade. Para realizar o ataque, o atacante pode mandar qualquer chave criptografada para a chave, em seguida a chave irá descriptografar o comando recebido e trocará o valor da chave que possui pelo valor recebido no comando. Então, ao tentar utilizar a chave com o novo valor ela ficará inutilizável.

- *Replay Attack on Authentication*

  De acordo com o protocolo, uma chave não gera números pseudoaleatórios, ela apenas reusa o que foi gerado pelo leitor. Logo, os comandos de autenticação enviados pelo carro podem ser gravados para uso futuro. A autenticação mútua proposta só autentica o carro na chave e verifica a origem dos dados da resposta da key fob para o carro.

- *Spoofing Attack on Memory Access Protection*

O comando “Write Memory Access Protection” ocorre sem autenticação. A partir dessa falha, um atacante pode alterar parte da memória da key fob prejudicando alguma funcionalidade.

- *Hijacking Communication Sessions*
  Como não há um *timestamp* ou um *cookie* de sessão, um atacante pode interceptar comandos entre chave e veículo, após uma autenticação bem-sucedida. Então, ele pode utilizar comandos de forma similar ao realizado no *Replay Attack*, onde comandos são armazenados para uso futuro.

3.9 CONSIDERAÇÕES FINAIS

Nesse Capítulo foram apresentados 9 sistemas de entrada e partida em automóveis, com cinco requisitos ligados à segurança, às vulnerabilidades e aos ataques existentes a partir de uma Revisão Sistemática e uma Revisão Exploratória.

Dentre as vulnerabilidades e ataques expostos nesse Capítulo, pode-se notar que as maiores falhas de segurança encontradas são devidas a erros de projeto na elaboração do sistema: chave fraca, algoritmo proprietário fraco, ausência de gerador de números pseudoaleatórios, comandos que são executados sem precisar de autenticação, etc.

Apesar das falhas encontradas, nota-se também que para se ter um sistema mais seguro não é preciso criar novos algoritmos e novas tecnologias, mas é preciso ser feito escolhas corretas de projeto do sistema. Um exemplo disso está na adoção do AES, que é utilizado no Open Software Immobilizer Stack da Atmel e que não apresentou falhas no que tange a questão da criptografia. Um outro bom exemplo que podemos citar é o uso da autenticação mútua, que garante que a troca de informações entre as partes do sistema só será feita uma vez que ambos reconhecem um ao outro. Além disso, ainda podemos destacar a tendência do uso do celular como algo benéfico, pois propcia uma maior capacidade de processamento, possibilitando, por exemplo, o uso de uma chave maior.

O próximo Capítulo apresenta um modelo de segurança para PKES que teve como guia os requisitos, os ataques e as vulnerabilidades apresentados nesse capítulo.

4 MODELO DE SEGURANÇA DE PKES

Neste capítulo é apresentado um modelo de PKES baseado no uso de smartphones que tem como principal objetivo a segurança.

4.1 INTRODUÇÃO

Um veículo durante sua vida útil passa pelos mais variados cenários de uso. Dentro desses cenários, existem alguns que se repetem com mais frequência e/ou são considerados mais relevantes do ponto de vista de uso do veículo (Figura 20). Durante toda essa vida útil, espera-se que o veículo seja seguro do ponto de vista da vida daqueles que utilizam o veículo como no caso de acidentes (equivalente ao termo em inglês, *safety*), e seguro do ponto de vista de roubos e furtos (equivalente ao termo em inglês, *security*).

No contexto de pesquisa desse trabalho, esse capítulo propõe um modelo de segurança de PKES com o foco no conceito de segurança da informação, ou seja, do termo em inglês *security*. Esse modelo tem como objetivo abranger todos os cenários da Figura 20 que serão abordados na Seção 4.3. Além disso, seguindo a tendência na área de PKES, esse modelo será elaborado a partir do uso do celular como dispositivo que contém a chave virtual do veículo, que se comunicará como o veículo através de BLE (*bluetooth low energy*).

Figura 20 - Ciclo de vida de um veículo - possíveis cenários

Fonte: o autor (2019)

4.2 REQUISITOS

O modelo proposto tem como objetivo principal ser um modelo seguro, do ponto de vista de segurança da informação. Porém, outros objetivos também foram considerados para que o sistema proposto seja viável do ponto de vista de uso. A seguir, considerando os objetivos de segurança e o melhor uso possível, são listados requisitos em ordem de prioridade:

- **Controle de acesso**
  Somente usuários autenticados devem ter acesso ao veículo.
- **Performance**
  O tempo máximo para abrir e fechar o automóvel deve ser imperceptível para o usuário, assim como o tempo para ligar o automóvel.
- **Abrir e fechar remotamente**
  O usuário poderá abrir e fechar o veículo remotamente dentro de uma distância máxima estabelecida.
- **Compartilhar o veículo**
  O proprietário poderá, se assim desejar, compartilhar chaves com outros usuários, mas para isso é preciso que eles estejam próximos ao veículo para que a chave temporária seja inserida no veículo.
- **Controle de acesso orientado a tempo e a localização**
  Usuários só podem ter acesso ao veículo dentro das limitações de localização e tempo configuradas pelo proprietário.

Como dito anteriormente, diante dos diversos cenários possíveis para um automóvel no que se refere a entrada e partida sem chaves, o modelo proposto foca em segurança de veículos baseado em *smartphones* como portador da chave virtual. Apesar de ser possível realizar transferências de chaves virtuais através da internet, esse requisito foi removido para evitar diversos problemas de segurança com o compartilhamento remoto, como por exemplo, o comprometimento da rede de comunicação entre proprietário e usuário.

4.3 ESCOPO

Diante de uma tendência na área de migrar para uso de celulares como portadores da chave[17], esse modelo será baseado em *smartphones*.

Como dito anteriormente, são muitos os cenários os quais um automóvel será submetido durante toda sua vida útil. O trabalho aqui apresentado foca apenas nos cenários de veículos particulares. Logo, faz parte do escopo negativo desse modelo os veículos corporativos, de locadoras ou de sistemas de compartilhamento. Apesar disso, alguns dos cenários existentes para carros corporativos podem facilmente ser resolvidos com o modelo proposto ou com pequenos ajustes. Além desses cenários, o celular com bateria descarregada também faz parte do escopo negativo do modelo.

Apesar do modelo proposto focar em segurança, de nada adiantaria, por exemplo, um veículo que levasse alguns poucos segundos para destravar as portas ou que levasse o usuário a memorizar e digitar senhas para abrir porta e dar partida no automóvel. Então, apesar de não ser o foco principal do trabalho em questão, aspectos de usabilidade e desempenho foram levados em consideração na elaboração do modelo, mas estes aspectos podem ser melhor explorados em trabalhos futuros.

Diante do exposto, os seguintes cenários serão tratados pelo modelo:

- Aquisição do automóvel
    - Exemplo: o veículo se encontra de posse da concessionária e acaba de ser adquirido pelo novo proprietário.
    - Objetivo: a concessionária, através da montadora, possui acesso à base de dados da chave do veículo, mas precisa transferi-la ao novo proprietário de forma permanente.
    - Desafio: Após a transferência, apenas o proprietário deverá ter acesso ao veículo. A montadora deverá ter armazenada uma chave reserva para uso emergencial e futuro.
- O uso das funções básicas de um sistema de controle de entrada e partida
    - Exemplo: O usuário de um veículo precisa usar as funções básicas de um veículo (travar as portas, destravar as portas, ligar o carro, abrir o porta-malas).

[17] https://www.reuters.com/article/us-autoshow-frankfurt-keys/bmw-says-car-keys-may-be-replaced-by-mobile-phone-apps-idUSKCN1BQ1ES

    - Objetivo: Autenticar o usuário antes de abrir a porta, abrir o porta-malas e antes de ligar o automóvel.
    - Desafio: A autenticação deve ser feita de modo que o usuário não tenha que ficar esperando para efetuar a ação. O tempo para que a autenticação aconteça não deve ser perceptível ao usuário. Além disso, apenas usuários autorizados poderão realizar tais ações.
- Compartilhamento do veículo em um domicílio
    - Exemplo: um casal de recém-casados adquiriu um carro, apesar de ambos dirigirem, eles só têm um carro e este é compartilhado.
    - Objetivo: o veículo precisa ter mais de uma chave ou os proprietários precisam usar a mesma chave.
    - Desafio: evitar a captura da réplica da chave por um intruso, dado que a chave tem os mesmos poderes da chave utilizada pelo proprietário.
- O uso do veículo em uma oficina e/ou lava jato
    - Exemplo: o veículo está com defeito e precisa ser levado a uma oficina. O carro irá pernoitar na oficina para que o serviço seja concluído e durante esse tempo o mecânico irá precisar ligar o veículo para testes.
    - Objetivo: uma chave temporária precisa ser compartilhada com o mecânico.
    - Desafio: essa chave será usada para ligar e desligar o veículo e fazer pequenos deslocamentos, mas essa chave não pode compartilhar novas chaves. Além disso, o carro não precisa sair da oficina e a chave precisa ficar em posse do mecânico até o dono retirar o veículo da oficina.
- Estacionamento com manobrista
    - Exemplo: o proprietário foi a um restaurante ou hotel no qual é oferecido um serviço de manobrista.
    - Objetivo: o proprietário precisa compartilhar uma chave temporária com o manobrista, mas, por segurança, essa chave não deverá ser usada além do estacionamento desse local, nem após o proprietário do veículo sair do estabelecimento com o carro. Além disso, essa chave não deverá ter permissão de ser compartilhada ou compartilhar novas chaves.

    - Desafio: essa chave será usada para ligar e desligar o veículo e fazer pequenos deslocamentos, mas não pode compartilhar novas chaves.
- Troca de aparelho
    - Exemplo: o proprietário adquiriu um novo aparelho celular e vendeu o aparelho antigo a um desconhecido.
    - Objetivo: o dono precisa transferir as chaves que estão no aparelho antigo para o novo. Essa troca deve inutilizar as chaves do aparelho antigo.
    - Desafio: Com o aparelho antigo não deverá ser possível acessar o veículo e o novo aparelho deve manter as mesmas permissões do aparelho antigo.
- Perda de aparelho celular
    - Exemplo: o aparelho celular do proprietário foi roubado e o dono do automóvel comprou um novo aparelho.
    - Objetivo: o dono precisa de uma nova chave no aparelho novo. Além disso, a chave do aparelho antigo deverá ser invalidada.
    - Desafio: Com o aparelho antigo não deverá ser possível acessar o veículo e o novo aparelho deve manter as mesmas permissões do aparelho antigo.
- Venda do veículo
    - Exemplo: O proprietário decidiu comprar um novo automóvel e vendeu o automóvel antigo a um amigo, porém, ambos moram em uma cidade muito pequena e distante de uma concessionária autorizada.
    - Objetivo: o novo dono deverá receber a chave com todas as permissões e o antigo dono deverá ter o acesso negado.
    - Desafio: a transferência tem que ser feita sem o deslocamento para a concessionária. Além disso, por questões de segurança e privacidade, o novo proprietário quer remover o acesso do antigo dono ao veículo.

4.4 ESCOPO NEGATIVO

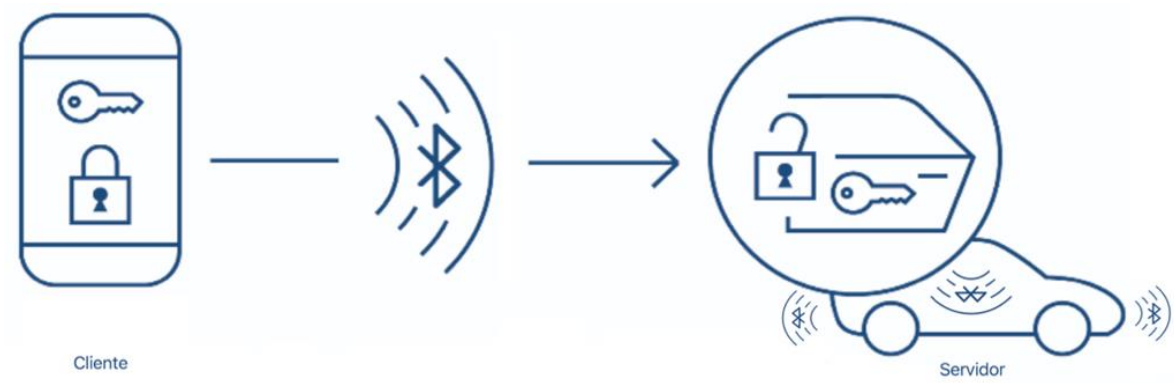
Apesar de focar em diversos cenários de uso de um sistema de entrada e partida sem chaves, essa pesquisa limitou-se aos cenários descritos na Seção 4.3. Então, não fazem parte do escopo dessa pesquisa os seguintes cenários:

- Sistema de compartilhamento de veículos (ex. Uber);
- Frota corporativa;
- Locadora de veículos;
- Celular descarregado;

4.5 ARQUITETURA

O modelo proposto é composto por duas partes, celular e veículo, formando uma rede bluetooth com uma arquitetura cliente-servidor (Figura 21). Ambas as partes possuem chaves de segurança compartilhadas para autenticação e criptografia das mensagens. O veículo contém antenas internas e externas que são utilizadas para detectar a presença do *smartphone* (chave) no interior e exterior do veículo.

Figura 21 - Visão geral

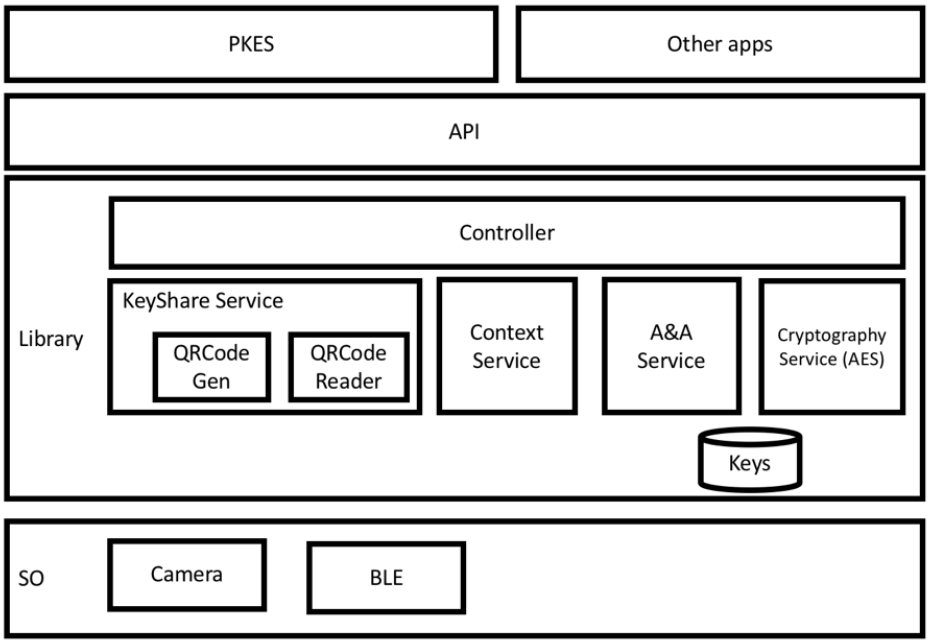


Fonte: O autor (2019)

4.5.1 Arquitetura da aplicação mobile

A proposta para o celular é que seja criada uma biblioteca para expor uma API (Application Programming Interface) utilizada em aplicações de PKES podendo conter uma interface para o usuário que seja customizável para atender os mais diversos modelos fabricados por uma montadora. Além disso, essa biblioteca também poderia ser utilizada por outros aplicativos criados pela montadora, caso necessário.

Figura 22 - Arquitetura – lado celular (cliente)



Fonte: O autor (2019)

- **PKES**

  É a aplicação *mobile* em si. Esse módulo contém a interface do usuário e faz uso da API para realizar chamadas e subscrever a eventos emitidos pela API. Através da interface do usuário é possível travar e destravar portas, compartilhar chaves, remover acesso de chaves e destravar porta-malas.

- **Other apps**

  Representa possíveis aplicações que façam uso da biblioteca via API. Exemplos: aplicações que identificam a presença do usuário nas proximidades do veículo e customizam o automóvel de acordo com as preferências do usuário (ajuste de volante, temperatura, músicas, trajetos do GPS).

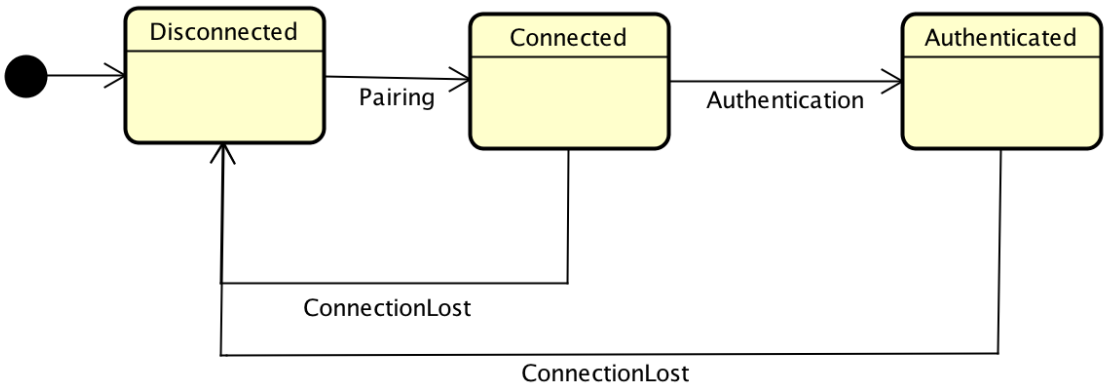
- **API**

  É a API (*Application Programming Interface*) que a biblioteca expõe para que outras aplicações e a aplicação de PKES utilizem os serviços que ela provê.

- **Controller**

  Esse módulo é o responsável por receber as chamadas da API e as executa-las. Ele contém uma máquina de estados para controle da aplicação. Essa máquina de estados da aplicação *mobile* é simples e contém os estados: Disconnected, Connected e Authenticated (Figura 23).

Figura 23 - Máquina de estados da aplicação *mobile*



Fonte: O autor (2019)

O estado Disconnected é quando o celular está sem conexão *bluetooth* com o veículo. Quando o acontece o pareamento, o estado é o Connected e após autenticação o estado é o Authenticated. Se em quaisquer estados a conexão for perdida (ConnectionLost) a máquina de estados retorna ao estado Disconnected.

- **KeyShare Service**

  É o modulo responsável pelo serviço de compartilhamento das chaves virtuais. Através desse módulo as informações da chave virtual são geradas ou lidas através de um QRCode.

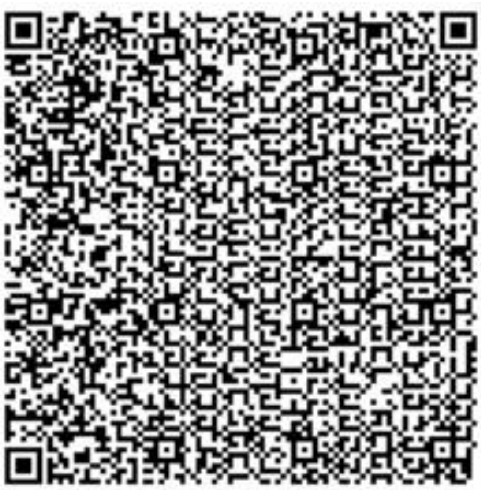
  - **QRCode Gen**

    Esse módulo pertence ao KeyShare e é responsável por gerar um QRCode com as informações das chaves (Figura 24). O QRCode é um meio de compartilhar a chave e as informações entre os usuários do veículo. As informações contidas no QRCode contemplam:

    - Chave do veículo 128 bits: é a chave usada na autenticação do carro. Esse tamanho de chave é o mesmo utilizado pelo Open Immobilizer Software Stack da Atmel (ATMEL, 2012) e que também é recomendado pelo governo dos Estados Unidos (BARKER; DANG, 2015)
    - Chave do aplicativo 128 bits: é a chave usada para autenticação do celular
    - Durabilidade da chave: tempo que a chave é válida
    - Localização: coordenadas geográficas que limitam o uso das chaves.
    - Identificador do veículo: 128 bits (UUID – Universally Unique Identifier)
    - Identificador da chave: 128 bits (UUID)

- PIN Bluetooth: senha para conectar com o bluetooth do veículo
- Posição do veículo: a última posição registrada do veículo.

Figura 24 - Exemplo de chave virtual



Fonte: O autor (2019)

As chaves do carro e do aplicativo compartilhadas através do QRCode serão utilizadas para a autenticação mútua. O identificador do veículo e da chave servem para o processo de autenticação e são utilizados para que a chave possa reconhecer o veículo antes de iniciar a autenticação e o veículo reconheça a chave. A durabilidade e a geolocalização são utilizadas para limitar as chaves temporárias. Já o PIN Bluetooth será utilizado no pareamento bluetooth entre celular e carro. A posição do veículo é utilizada na autenticação ciente de contexto.

- **QRCode Reader**

  Esse módulo pertence ao KeyShare e é responsável por ler os QRCodes recebidos através da câmera e armazenar as informações recebidas no módulo Keys.

- **Context Service**

  Esse módulo é o responsável por inferir a última posição do veículo e a posição atual da chave.

- **A&A Service**

  Esse módulo é o responsável pela autenticação e autorização do sistema. A autenticação se dá de forma mútua e ciente de contexto (Seção 4.6). Já a autorização é baseada no modelo ABAC (Attribute Based Acces Control) uma vez que as chaves possuem atributos de tempo e geolocalização para permitir o uso do automóvel com chaves temporárias.

- **Cryptography Service**

Esse módulo contém o algoritmo de criptografia AES (Advanced Encryption Standard), sendo responsável por criptografar e descriptografar as mensagens que são trocadas entre veículo e celular. Esse módulo utiliza chave de 256 bits para cifrar as mensagens.

- **BLE**

  Através desse módulo, a aplicação se conecta com o veículo para formar uma rede *bluetooth* de baixo consumo de energia (BLE – Bluetooth Low Energy) por onde as mensagens serão trocadas entre aplicação e veículo.

- **Camera**

  A câmera do *smartphone* será usada pelo QRCode Reader para leitura do QRCode que contém as informações da chave virtual.

- **Keys**

  Esse módulo armazena as chaves, os identificadores e as permissões que as chaves possuem. Existem quatro tipos de chaves no modelo proposto:

  - **Chave global fixa**

    É a chave que fica em poder da montadora. Essa chave tem a permissão de executar quaisquer comandos.

  - **Chave proprietária**

    É a chave que fica com os proprietários dos veículos. Essa chave tem a permissão de executar quaisquer comandos, exceto UpdateKey na chave global fixa.

  - **Chave temporária com permissão de compartilhamento**

    Para uso temporário, essa chave tem permissão para executar todos os comandos exceto UpdateKey na chave global fixa, na chave proprietária e em si mesma.

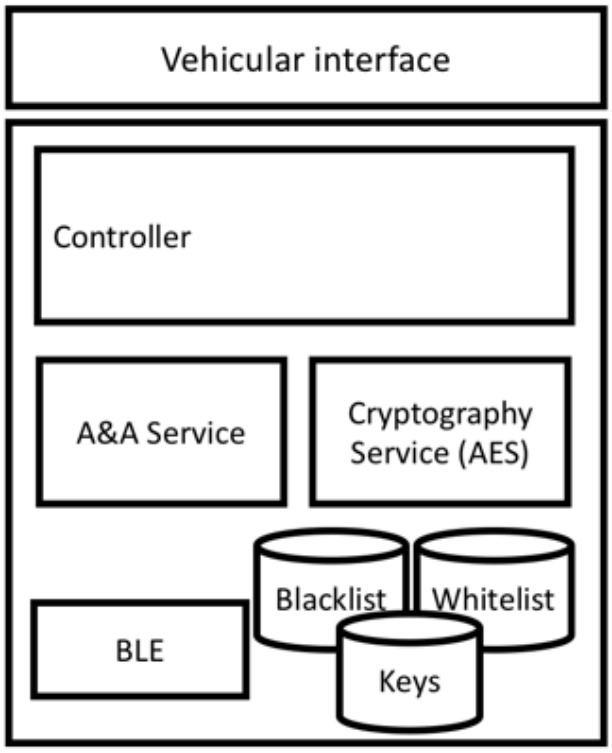
  - **Chave temporária sem permissão de compartilhamento**

    Também de uso temporário, essa chave tem permissão de executar todos os comandos, exceto UpdateKeys. A diferença entre a chave temporária com permissão de compartilhamento para a chave temporária sem permissão de compartilhamento é que a primeira é indicada para uso de um amigo e a segunda de um prestador de serviço. Ao emprestar o carro a um amigo ele pode, eventualmente, precisar compartilhar a chave com um prestador de serviço como, por exemplo, um manobrista. Já o manobrista, não precisa da permissão para compartilhar chave.

4.5.2 Arquitetura da Aplicação do Carro

A arquitetura contida no carro possui módulos semelhantes aos existentes no celular. Por outro lado, essa arquitetura não contém uma API onde uma aplicação mobile envia comandos, mas deve ter uma interface de comunicação para executar os comandos de travar/destravar portas e porta-malas e autenticar no imobilizador e uma interface de comunicação BLE para se conectar com a aplicação.

Figura 25 - Arquitetura – lado do veículo (servidor)



Fonte: O autor (2019)

- ***Vehicular interface***

  Esse módulo é o responsável pela comunicação entre o cliente PKES e o veículo. Através dele os comandos (Seção 4.5) são repassados ao veículo.

- ***Controller***

  O Controller é o módulo responsável por coordenar as ações no veículo. Ele possui uma máquina de estados idêntica a do celular.

- ***A&A Service***

  O A&A Service é o responsável pela autenticação mútua e autorização. Ele contém os mesmos elementos do módulo presente no celular para que seja realizada o processo de autenticação e autorização.

- ***Cryptographic Service***

  Esse módulo deve conter a implementação do algoritmo AES e é responsável por criptografar e descriptografar as mensagens trocadas.

- ***Keys***

  Módulo responsável por armazenar as chaves juntamente com identificadores e permissões. Cada chave possui um identificador único associado e esse identificador é utilizado como resposta ao comando ReadUUID. Nesse módulo estarão contidas as chaves do proprietário, as chaves temporárias e a chave mestra da montadora.

- ***Blacklist***

  Contém os *MAC Address bluetooth* que excederam o limite de tentativas de conexões ou dos smartphones cujas chaves expiraram o tempo de uso previsto. Essa estratégia é utilizada para evitar ataques de *denial of service*.

- ***Whitelist***

  Contém os *MAC Address bluetooth* dos smartphones que podem usar o veículo e os UUIDs válidos.

- **BLE**

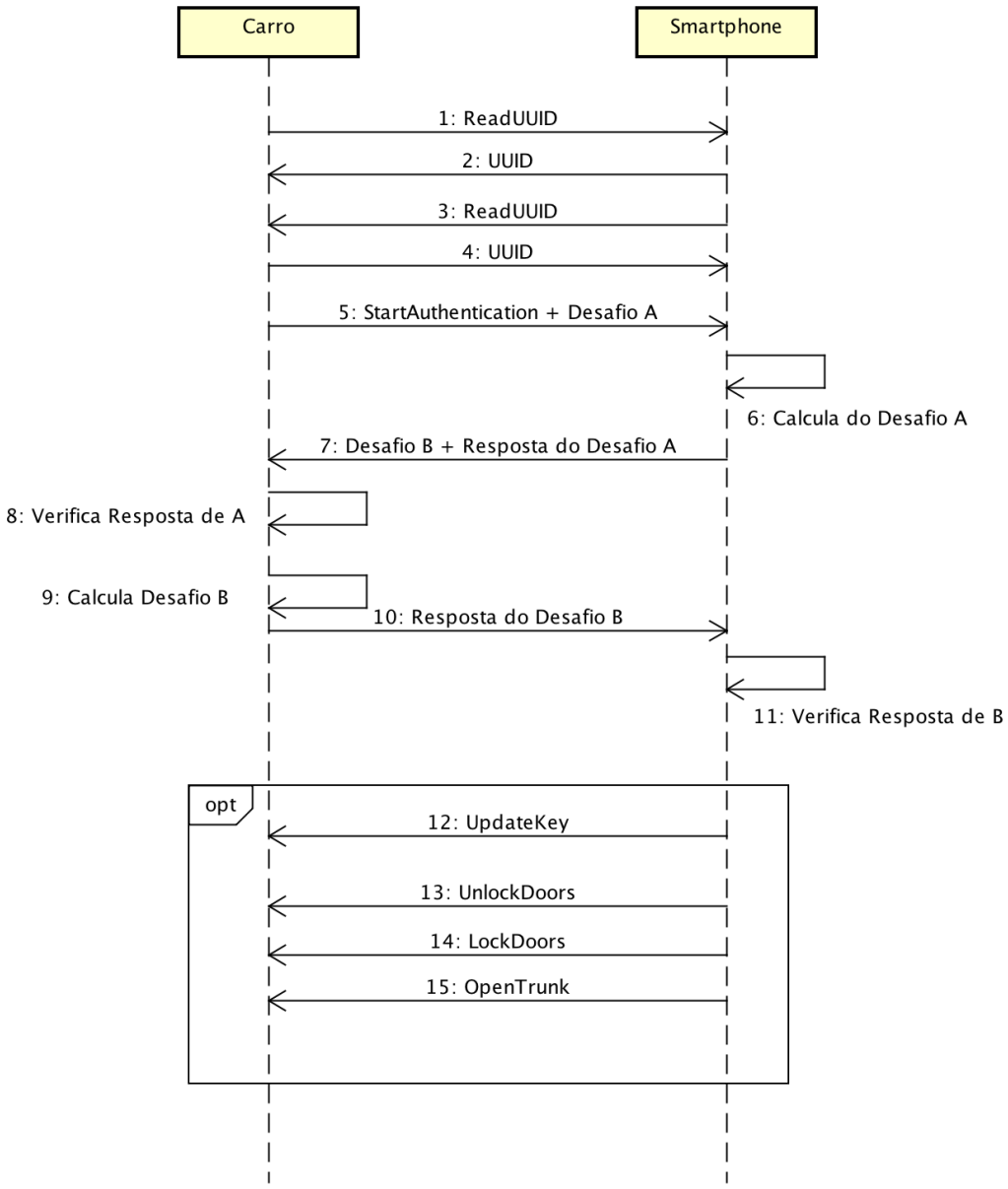
  É o módulo que implementa o *bluetooth low energy* no veículo. Através dessa interface de comunicação, veículo e celular formam uma rede na qual os comandos serão trafegados.

4.6 PROTOCOLO DE COMUNICAÇÃO

O protocolo de comunicação entre celular e carro é baseado em mensagens. O celular envia a mensagem para o carro que responde após um determinado período de tempo e vice-versa.

Para efetuar ações como, por exemplo, travar portas ou ligar o veículo é preciso que veículo e chave estejam devidamente autenticados, além disso, também é necessário que comandos sejam disparados para que a ação seja efetuada (no caso de entrada e saída da zona de travamento, o veículo efetua essas ações sem interação com o dispositivo-usuário). A Figura 26 ilustra a troca de mensagens entre carro e *smartphone* para a autenticação, sendo as últimas mensagens comandos opcionais disparados explicitamente pelo dispositivo-usuário.

Figura 26 - Autenticação sem ciência de contexto



Fonte: O autor (2019)

As mensagens existentes no modelo são:

- **ReadUUID**

  Comando ReadUUID é o comando mais simples. Ele é utilizado para efetuar a leitura do identificador do veículo se ele for executado pelo celular. Já no caso dele ser utilizado pelo carro, ele é utilizado para leitura do identificador do celular. Esse comando precede o início da autenticação propriamente dita.

- **StartAuthentication**

  Esse é o comando utilizado para iniciar a autenticação de fato. Ele é composto pelo identificador do comando, o desafio e o resultado do desafio criptografado.

- **UnlockDoors**

  Esse é o comando utilizado para a abertura de portas de maneira explícita através do aplicativo. Da mesma maneira que os veículos possuem controle remoto nas chaves para abrir e fechar o veículo, o modelo proposto apresenta esse comando para abertura remota. Esse comando só pode ser efetuado de maneira autenticada.

- **LockDoors**

  Esse é comando é semelhante ao anterior, porém o intuito dele é travar as portas remotamente, quando o dispositivo-usuário sai do raio de comunicação com o veículo e após determinado tempo (ex. 5 segundos, podendo ser configurável) – Seçao 4.6.4. Assim como o comando de UnlockDoors, esse comando só pode ocorrer de maneira autenticada.

- **OpenTrunk**

  Similar aos comandos UnlockDoors e LockDoors, esse é comando utilizado para abrir a mala do veículo remotamente através do aplicativo.

- **EngineAuthentication**

  Esse é o comando realizado para autenticação e permitir que o motorista ligue o veículo. Esse comando é disparado automaticamente pelo veículo na medida que ele detecta a presença de uma chave no interior do veículo.

- **UpdateKey**

  Esse comando é utilizado para atualizar as chaves do veículo. Cada chave só poderá atualizar chaves com permissões inferiores ou iguais a ela. O objetivo desse comando é remover chaves temporárias que expiraram ou criar novas chaves que serão compartilhadas. Para que esse comando seja efetuado é necessário que a chave proprietária esteja autenticada.

4.7 FUNÇÕES

Essa seção explica como funcionam as funções do modelo proposto. Através dessas funções é possível cobrir os cenários abordados na Seção 4.3.

4.7.1 Configuração inicial da chave

Na configuração inicial da chave, a montadora precisa configurar a chave-mestra (chave global fixa) do veículo. O objetivo dessa chave é para usos emergenciais como, por exemplo, no caso de perda do celular do proprietário. Essa chave deve ser gerada de forma aleatória para cada veículo (GARCIA et al., 2016). Além disso, essa chave precisa ser criptografada no banco de dados da montadora para evitar o vazamento das chaves. A maneira como essa chave é armazenada foge

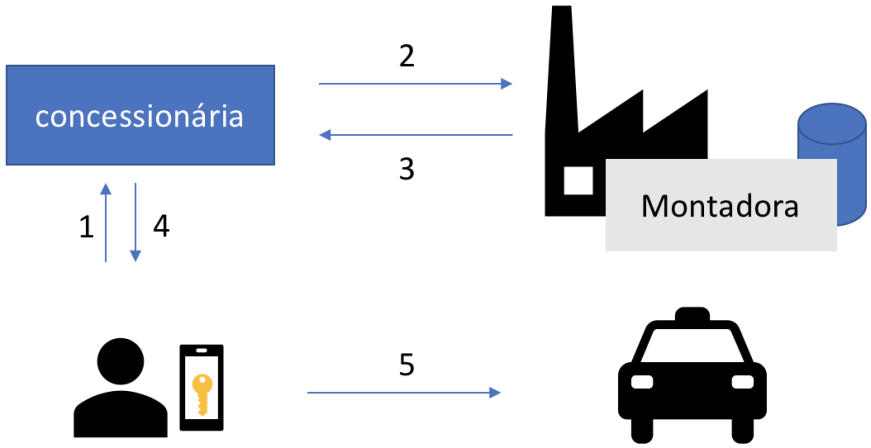
do escopo desse trabalho, mas ela deve ser armazenada de maneira segura e criptografada, a fim de não comprometer a segurança dos veículos e evitar um *recall* o que geraria um enorme prejuízo.

4.7.2 Aquisição do veículo

Ao adquirir o veículo na concessionária, o novo proprietário deverá receber a chave proprietária do veículo. Para isso, ele deve realizar os seguintes passos:

1. Realizar o cadastro na montadora através da concessionária e baixar o aplicativo;
2. Então, a concessionária deve requisitar a chave do veículo;
3. A montadora envia as chaves ao proprietário através da concessionária;
4. A concessionária configura a chave no celular do proprietário do automóvel (através da leitura do QRCode);
5. Proprietário se autentica no veículo normalmente.

Figura 27 - Configuração inicial da chave

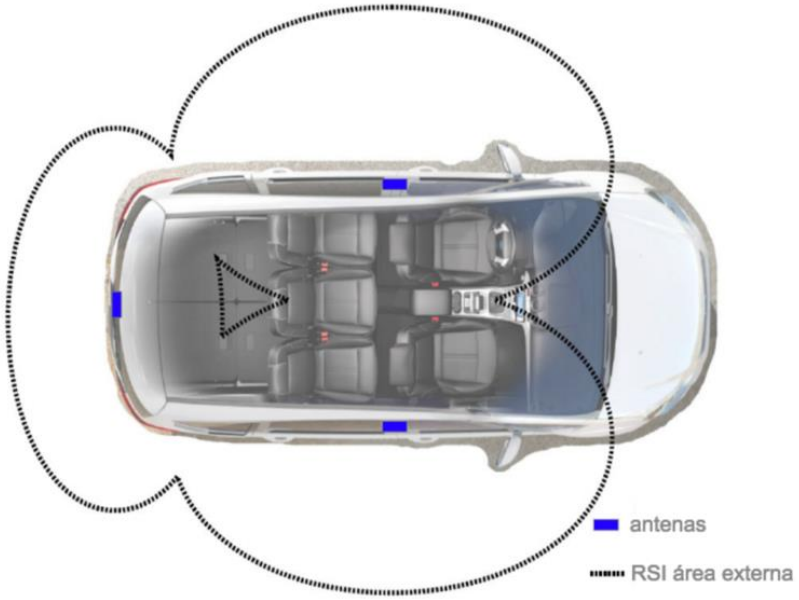


Fonte: O autor (2019)

4.7.3 Destravar portas e porta-malas

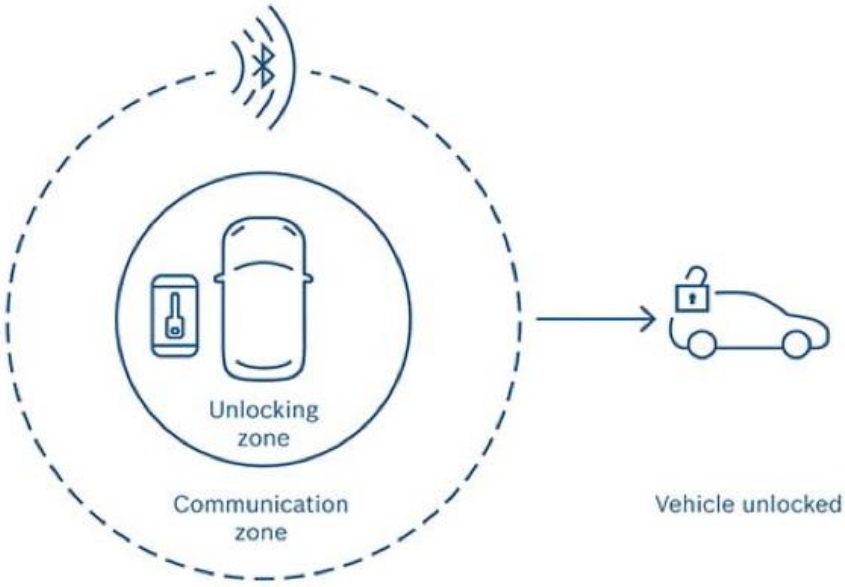
Para realizar a abertura das portas e do porta-malas o modelo utiliza antenas (Figura 28) no carro para detectar a proximidade da chave através da força do sinal (RSSI – Received Sinal Strengh Indication) do *bluetooth* (BLE) do celular. Quando o usuário se aproxima do veículo e entra na área de conexão, o veículo inicia o pareamento *bluetooth* com o celular. Após o pareamento, o veículo e o *smartphone* se identificam (ReadUUID) e iniciam o processo de autenticação mútua com o comando StartAuthentication. Uma vez autenticado, a porta é destravada (comando UnlockDoors) quando a chave se aproxima da área de destravamento (Figura 29). Essa funcionalidade é similar a que é utilizada no modelo da Bosch (BOSCH, [s.d.]) com o conceito de área de comunicação e de destravamento do veículo.

Figura 28 - Antenas externas



Fonte: Adaptada de Atmel (2012)

Figura 29 - Destravamento

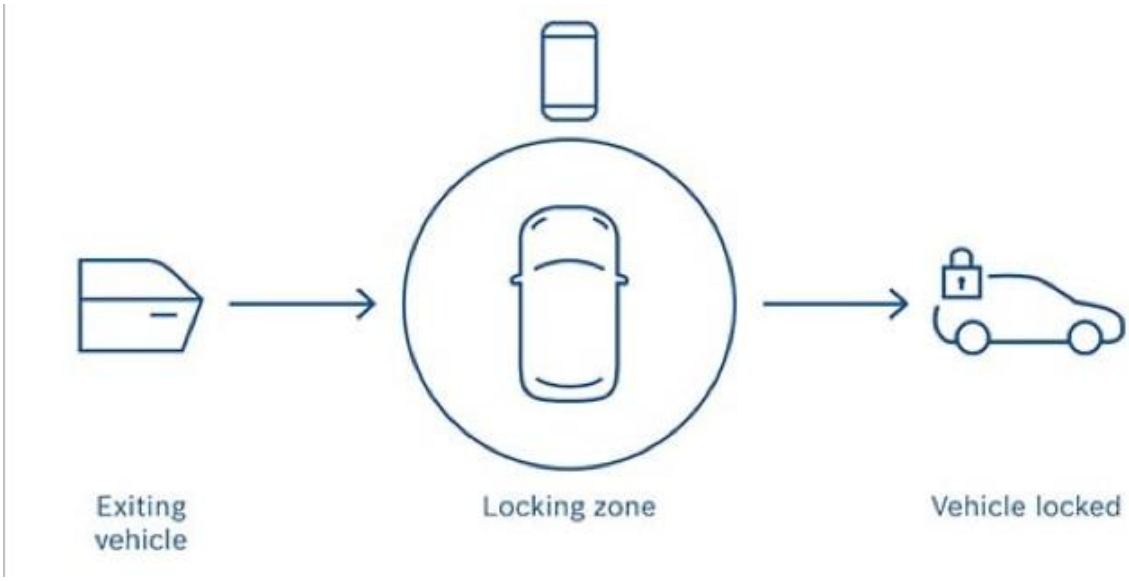


Fonte: Bosch [s.d.]

4.7.4 Travar portas e porta-malas

De maneira oposta ao que ocorre no destravamento, o comando de travamento ocorre quando um celular autenticado sai da zona de travamento do veículo (Figura 30). Os mesmos sensores utilizados para destravar são utilizados para travar na medida que o celular se afasta, a força do sinal diminui e o veículo é travado. Por medida de segurança, caso a conexão seja perdida em algum momento, as portas são travadas automaticamente ou quando o veículo começa a se locomover.

Figura 30 - Travamento

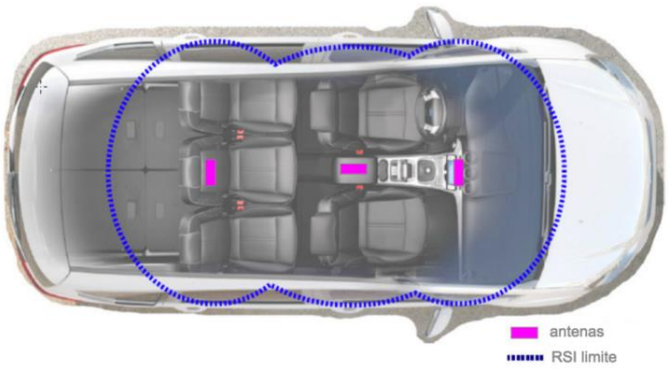


Fonte: Adaptada de Bosch [s.d.]

4.7.5 Ligar o veículo

Para ligar o veículo, o automóvel dispõe de antenas internas que detectam a presença da chave no interior do veículo através da medição da força do sinal bluetooth do celular (Figura 30). Uma vez que essa chave está no interior do veículo e é detectada e o carro inicia o processo de autenticação do motor. Para detectar a presença da chave no interior do automóvel, pode-se utilizar algum algoritmo de localização *indoor* para BLE como, por exemplo, o de Thaljaoui et al. (2015) que obteve um erro médio de 40 centímetros em ambientes de $4\mathrm{m}^2$. Após ser autenticado, o motorista precisar acionar o botão start/stop próximo ao volante do automóvel para ligá-lo (Figura 32). Para desligar o automóvel não é necessário estar autenticado.

Figura 31 - Antenas internas



Fonte: Adaptada de Atmel (2012)

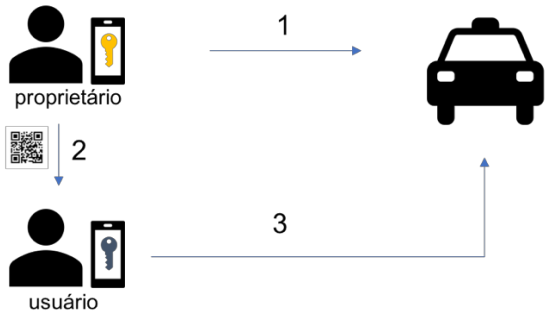
Figura 32 - Start/Stop engine

Fonte: O autor (2019)

4.7.6 Compartilhamento de chaves

Para compartilhar uma chave, o proprietário deve estar autenticado e configurar na aplicação *mobile* que tipo de chave será compartilhada (temporária com permissão de compartilhamento com terceiros ou sem permissão de compartilhamento). Essa configuração inclui todas as informações que o QRCode contém descritas na subseção 4.4.1. Após realizar essa configuração, o comando UpdateKey é disparado para inserir a chave temporária no módulo Keys do veículo junto com o Mac Address e o UUID no módulo de *whitelist* (1). Quando o comando UpdateKey for executado com sucesso, a aplicação apresentará um QRCode no aparelho através do KeyShare (2). Então, o usuário que vai receber a chave deverá fazer o escaneamento do QRCode para receber a chave virtual com as informações, e assim poder ser autenticado junto ao veículo proprietário (3).

Figura 33 - Compartilhamento da chave com usuário fisicamente próximo



Fonte: O autor (2019)

4.7.7 Remoção de chaves

Para a remoção de chaves o comando utilizado é o UpdateKey. No caso de uma aquisição de um novo *smartphone*, transferência do carro ou por quaisquer outras necessidades, o usuário poderá remover as chaves virtuais do veículo. Porém, todas

as chaves não podem ser removidas, o veículo tem que manter no mínimo uma chave de proprietário, além da chave da montadora. Para a remoção das chaves, o veículo efetua de tempos em tempos a validadação das chaves armazenadas e elimina as que ultrapassaram o prazo estimado. Além disso, antes de cada autenticação, ao ler o UUID da chave virtual o veículo pode remover a chave vencida e finalizar a conexão.

4.8 AUTENTICAÇÃO CIENTE DE CONTEXTO

Um dos principais ataques em PKES é o *relay attack* (FRANCILLON; DANEV; CAPKUN, 2011). Com o objetivo de mitigar esse tipo de ataque, o processo de autenticação do modelo proposto se dá de forma mútua (ou bilateral) e ciente de contexto. A autenticação é considerada mútua porque carro e *smartphone* autenticam um ao outro. Além disso, ela é ciente de contexto porque o celular só participa do processo de autenticação se ele inferir que está próximo ao veículo.

Para inferir que o *smartphone* está próximo ao veículo são necessárias duas informações: qual a última posição do veículo e se o *smartphone* está próximo. Para registrar a última posição do veículo, o celular precisa saber onde o carro foi estacionado desde o último uso. Para isso, as APIs de *smartphones* já contam com serviços que detectam se o usuário se encontra andando, correndo, dirigindo ou andando de bicicleta[18]. Esse tipo de informação associada com informações de outros sensores como, por exemplo, o de giroscópio e sensores de localização é possível, por exemplo, inferir que o motorista saiu do automóvel e começou a caminhar. Nesse momento, a posição do veículo é armazenada no celular como sendo a última posição conhecida.

Já para identificar se *smartphone* está próximo ao veículo é necessário usar sensores de localização e calcular se a posição atual é próxima a última posição do veículo. Então, caso o celular identifique que ele está próximo do veículo ele participa do processo de autenticação, caso contrário ele não participa.

Obviamente, o uso de informações contextuais para efetuar a autenticação aumenta a complexidade e tempo gasto para autenticar o usuário, porém como a segurança é o requisito de maior prioridade no modelo proposto, esse passo extra foi adicionado no processo prévio a autenticação.

Nos casos especiais em que o *smartphone* não consegue inferir que o usuário está próximo ao veículo ainda é possível utilizar os comandos UnlockDoors,

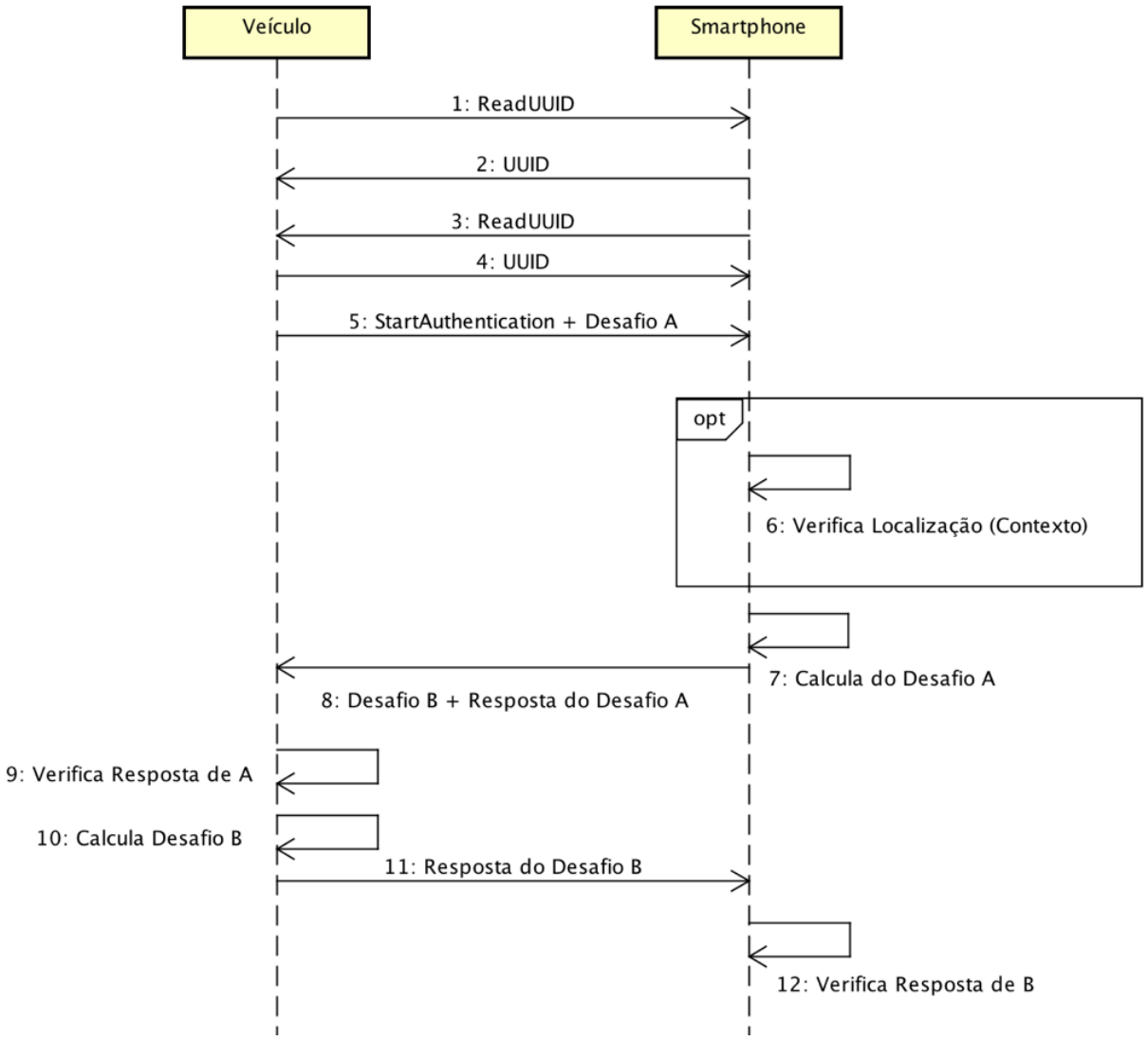
[18] https://developer.apple.com/documentation/coreml
https://developer.android.com/reference/

LockDoors e OpenTrunk através da *interface* da aplicação e, nesses casos, o módulo de contexto não é acionado durante a autenticação para verificar a localização.

O protocolo de autenticação conforme a Figura 34 ocorre da seguinte forma:

1. O veículo detecta a presença da chave e envia o comando ReadUUID para identificar a chave;
2. O *smartphone* envia o UUID;
3. O *smartphone* envia o comando ReadUUID para identificar o carro;
4. O veículo envia o UUID para o *smartphone*;
   (nesse ponto veículo e *smartphone* reconhecem o UUID um do outro)
5. O veículo envia o comando StartAuthentication ao *smartphone*;
6. Caso o *smartphone* esteja ciente de que está próximo ao veículo, ele calcula o desafio A (enviado pelo carro);
7. Em seguida, o *smartphone* envia a resposta ao desafio A, junto com um novo desafio;
8. O veículo verifica a resposta do desafio A;
   (nesse momento a chave está autenticada ao automóvel)
9. O veículo calcula o desafio B;
10. O veículo envia a resposta ao desafio B;
11. O *smartphone* verifica a resposta ao desafio B;
    (nesse momento o automóvel está autenticado ao smartphone)

Figura 34 - Autenticação Ciente de Contexto



Fonte: O autor (2019)

4.9 LIMITAÇÕES DO MODELO

O modelo de PKES proposto tem o foco em segurança e, por isso, apresenta algumas limitações. Esse modelo não considera todos os cenários possíveis dentro do ciclo de vida de um automóvel, como, por exemplo, os veículos corporativos, ou o cenário no qual o celular se encontra descarregado já que não haveria condições de estabelecer uma rede bluetooth sem o aparelho carregado. Além disso, esse modelo é idealizado para veículos particulares com os mais variados custos de produção e não considera que o automóvel disponha de um chip de telefonia móvel no veículo, que é comum em modelos top de linha, como por exemplo veículos da BMW que possuem o ConnectDrive (BMW, [s.d.]). Devido ao fato de focar em segurança, o modelo também não apresentou questões de usabilidade do sistema e custo de implementação, que é um requisito muito importante ao se tratar de uma produção em

escala. Outro ponto de limitação do modelo é o fato dele não ter sido implementado e testado. Essa implementação fica como um trabalho futuro.

4.10 CONSIDERAÇÕES FINAIS

Essa capitulo apresentou um modelo para entrada e partida passivas de veículos com foco em segurança e baseado em uma revisão de literatura. A Seção 4.2 apresentou os requisitos desde modelo, enquanto a Seção 4.3 detalhou o escopo do modelo proposto. Além disso, a Seção 4.4 apresentou a arquitetura do sistema do ponto de vista do veículo e da aplicação mobile. Já o protocolo de comunicação utilizado no modelo foi apresentado na Seção 4.5 e as funções na Seção 4.6. Na seção 4.7, foi apresentado a autenticação ciente de contexto. Por último, as limitações do modelo foram analisadas na Seção 4.8.

5 CONCLUSÃO

O último capítulo deste trabalho apresenta as considerações finais, os resultados obtidos relacionados com os objetivos iniciais da pesquisa, as possibilidades para realização de trabalhos futuros e as considerações finais do trabalho.

Com o avanço da tecnologia e a busca por comodidade, a presença de sistema de PKES tem se tornado cada vez mais comum nos veículos, inclusive nos de baixo custo. Porém, os sistemas existentes ainda apresentam diversas falhas de segurança tornando os veículos suscetíveis a roubos, o que causa prejuízo aos proprietários e montadoras.

Nesta dissertação teve-se como objetivos principais: apresentar o que vem sendo feito e estudado a respeito de controle de acesso e partida em veículos e apresentar um modelo PKES em veículos baseado em *smartphones* e com foco em segurança.

Diante de tais objetivos, as conclusões finais dessa dissertação são discutidas, são sugeridos possíveis trabalhos futuros para dar continuidade à pesquisa, bem como são apresentadas as principais limitações da pesquisa realizada.

5.1 CONTRIBUIÇÕES

As principais contribuições deste trabalho são a revisão da literatura e a proposta de um PKES que considera importantes requisitos de segurança para facilidade cada vez mais presente nos veículos atuais. A revisão sumariza o que vem sendo pesquisado pela indústria e comunidade científica a respeito de entrada e partida sem chaves. Além disso, a revisão serve como ponto de partida para novos estudos na área.

Já o modelo proposto vai ao encontro da tendência dos últimos tempos que é o uso do *smartphone* como chave virtual do veículo. Além disso, a arquitetura proposta é baseada no que já existe na literatura como, por exemplo, o uso de *bluetooth low energy* e o algoritmo AES, não se limitando ao uso dessas tecnologias caso algoritmos mais robustos venham a surgir ou novas tecnologias se sobreponham ao *bluetooth*.

O modelo proposto também faz o uso de ciência de contexto durante o processo de autenticação. O uso de informação contextual tem como principal objetivo tornar o sistema seguro ao *replay attack*.

5.2 TRABALHOS FUTUROS

De acordo com os resultados obtidos, pode-se esperar como uma continuação deste trabalho a implementação do modelo e a execução de testes de segurança para melhor avaliar o modelo proposto. Além disso, pode-se considerar como trabalho futuro o compartilhamento de chaves virtuais através da Internet e considerar cenários de carros corporativos, de locadoras e sistemas de compartilhamento de veículos. Outro aspecto possível a ser analisado como trabalho futuro é tornar o sistema ciente de contexto para criação de chaves temporárias. Além desses pontos, aspectos funcionais como, por exemplo, desempenho e usabilidade do sistema proposto também podem ser analisados em trabalhos futuros, bem como a comparação modelo proposto com outras soluções.

5.3 LIMITAÇÕES DO ESTUDO

Esse trabalho limitou-se a realizar uma revisão da literatura e a proposta de um modelo de controle de acesso e partida sem chaves para veículos. Não foi objeto de estudo apresentar detalhadamente todos as vulnerabilidades e ataques para cada sistema analisado na revisão da literatura, mas foi possível apresentá-los e, a partir disso, elaborar o modelo proposto.

O modelo focou, principalmente, em aspectos de segurança e parte dos cenários para controle de acesso e partida em veículos particulares. Esse modelo teve como objetivo abranger os principais cenários existentes para o uso de automóveis particulares e desconsiderou cenários de frota de veículos corporativos, sistemas de compartilhamento de veículos e locação de veículos, além do celular descarregado. Além disso, ele limitou-se a um modelo teórico baseado no que já existe na literatura, não havendo, portanto, uma implementação e testes de segurança para o sistema aqui proposto.

5.4 CONSIDERAÇÕES FINAIS

A necessidade de sistemas seguros de controle de acesso e partida em veículos é notória. Os trabalhos publicados pela comunidade científica e as matérias da mídia somados às estatísticas sobre roubos de veículos evidenciam que os PKES ainda precisam evoluir para ser considerados seguros.

Então, a fim de evitar prejuízos tanto por parte das montadoras como dos donos de veículos, é fundamental o investimento em sistemas que utilizem algoritmos de criptografia testados pela comunidade científica com chaves maiores e protocolos confiáveis, como o apresentado no modelo proposto. O sistema proposto aponta uma possibilidade para a criação de sistemas de PKES mais seguros.

REFERÊNCIAS

AL-MUHTADI, J. et al. Cerberus: a context-aware security scheme for smart spaces. In: PROCEEDINGS OF THE FIRST IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS, 2003. (PERCOM 2003).

AL-SARAWI, Shadi et al. Internet of Things (IoT) communication protocols: Review. In: 2017 8TH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY (ICIT) 2017.

AS/NZS. **AS/NZS 4601:1999 - Vehicle immobilizers**. Disponível em: <https://www.saiglobal.com/PDFTemp/Previews/OSH/as/as4000/4600/4601.pdf>. Acesso em: 5 jul. 2018.

ATMEL. **Atmel ATA5580 - The AES 125kHz Transponder with Open Immobilizer Software Stack**. 2012. Disponível em: <https://www.mouser.com/ds/2/36/doc9254-33290.pdf>. Acesso em: 5 jul. 2018.

BARDRAM, Jakob E.; KJÆR, Rasmus E.; PEDERSEN, Michael Ø. Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing. In: [s.l: s.n.]. p. 107–123.

BARKER, Elaine B.; DANG, Quynh H. Recommendation for Key Management Part 3: Application-Specific Key Management Guidance. **NIST Special Publication 800-57**, [s. l.], p. 1–142, 2015. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf>

BENADJILA, Ryad et al. One Car , Two Frames : Attacks on Hitag-2 Remote Keyless Entry Systems Revisited. In: USENIX WOOTS 2017.

BLUETOOTH SPECIAL INTEREST GROUP (SIG). **Bluetooth Core Specification Version 5.0** 2016.

BMW. **BMW Connect Drive Services**. [s.d.]. Disponível em: <https://www.bmw.ie/en/topics/owners/for-owners/connecteddrive-forusers/connecteddrive-info.html>. Acesso em: 6 jun. 2018.

BOGDANOV, Andrey. Cryptanalysis of the KeeLoq block cipher. **IACR Cryptology ePrint Archive**, [s. l.], v. 2007, p. 55, 2007. Disponível em: <https://pdfs.semanticscholar.org/b945/3b128260f92d77450c0a6b7b018029b58ac4.pdf%0Ahttp://dblp.uni-trier.de/db/journals/iacr/iacr2007.html#Bogdanov07>

BONO, Stephen et al. Security Analysis of a Cryptographically-Enabled RFID Device. In: 14TH USENIX SECURITY SYMPOSIUM 2005, Berkeley, CA, USA. USENIX Association, 2005.

BORGIA, Eleonora. **The internet of things vision: Key features, applications and open issuesComputer Communications**, 2014.

BORST, Johan; PRENEEL, Bart; VANDEWALLE, Joos. On the time-memory tradeoff between exhaustive key search and table precomputation. In: SYMPOSIUM ON INFORMATION THEORY IN THE BENELUX 1998.

BOSCH. **Perfectly keyless**. [s.d.]. Disponível em: <https://www.bosch-mobility-solutions.com/en/products-and-services/mobility-services/perfectly-keyless/>. Acesso em: 1 jul. 2018.

BOUKERCHE, Azzedine; NAKAMURA, Eduardo. Localization systems for wireless sensor networks. **IEEE Wireless Communications**, [s. l.], v. 14, n. 6, p. 6–12, 2007. Disponível em: <http://ieeexplore.ieee.org/document/4407221/>

BUDGEN, David; BRERETON, Pearl. **Performing systematic literature reviews in software engineeringProceeding of the 28th international conference on Software engineering - ICSE '06**.

CARATTO, D.; PIAZANNO, C.; GINEVRO, S. **System for passive entry and passive start for a motor vehicle**, US9045102B2, 2015.

CHAI, S.; AN, R.; DU, Z. An Indoor Positioning Algorithm Using Bluetooth Low Energy RSSI. **Amsee**, p. 276–278, 2016.

CHIH-NENG, Liang; HUANG-BIN, Huang; BO-CHIUAN, Chen. Fingerprint Identification Keyless Entry System. **Proceedings of World Academy of Science: Engineering & Technology**, [s. l.], v. 46, p. 44–49, 2008.

CNET. **Apple, Audi, BMW agree on standard for using smartphones as car keys**. 2018. Disponível em: <https://www.cnet.com/roadshow/news/2018-car-connectivity-consortium-smartphone-car-keys-bmw-audi-apple-samsung/>. Acesso em: 9 jul. 2018.

CONTINENTAL. **No Title**. [s.d.]. Disponível em: <http://continental-carkey.com/>. Acesso em: 1 jul. 2018.

COURTOIS, Nicolas T. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In: **CRYPTO 2003: Advances in Cryptology** v. 2729p. 176–194.

COURTOIS, Nicolas T.; O'NEIL, Sean; QUISQUATER, Jean Jacques. Practical algebraic attacks on the hitag2 stream cipher. In: SAMARATI, Pierangela et al. (Eds.). **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. v. 5735 LNCSp. 167–176.

COVINGTON, Michael J. et al. A context-aware security architecture for emerging applications. In: PROCEEDINGS - ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, ACSAC 2002,

DEY, Anind K. Understanding and using context. **Personal and Ubiquitous Computing**, [s. l.], v. 5, n. 1, p. 4–7, 2001.

EC. **Commission Directive 95/56/EC of 8 November 1995 adapting to technical progress Council Directive 74/61/EEC relating to devices to prevent the unauthorized use of motor vehicles**.

ECKERMANN, E. **World History Of The Automobile**. Society of Automotive Engineers, 2001.

EISENBARTH, Thomas et al. On the power of power analysis in the real world: A

complete break of the KeeLoq code hopping scheme. In: LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS) 2008.

FISHER, Bill et al. Attribute Based Attribute Based - Approach, Architecture, and Security Characteristics. **Nist Special Publication 1800**, 2016.

FRANCILLON, Aurelien; DANEV, Boris; CAPKUN, Srdjan. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. **Network and Distributed System Security Symposium**, p. 431–439, 2011.

GARCIA, Flavio D. et al. Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems. **Proceedings of the 25th USENIX Security Symposium**, p. 929--944, 2016.

GOMEZ, Carles; OLLER, Joaquim; PARADELLS, Josep. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. **Sensors (Switzerland)**, v. 12, n. 9, p. 11734–11753, 2012.

GUARD, Bloodspear Laboratories; Nexus. Universal DDoS Mitigation Bypass. **Black Hat USA 2013**, 2013.

IATROU, Dimitrios. **Context Aware Access Control**. 2017. Dinamarca: Dissertação de Mestrado - Technical University of Denmark, 2017.

INDESTEEGE, S. et al. A practical attack on KeeLoq. **Eurocrypt 2008**, p. 1–18, 2008.

JALALI, Samireh; WOHLIN, Claes. Systematic literature studies. In: PROCEEDINGS OF THE ACM-IEEE INTERNATIONAL SYMPOSIUM ON EMPIRICAL SOFTWARE ENGINEERING AND MEASUREMENT - ESEM ’12 2012.

JIANYONG, Zhu et al. RSSI based Bluetooth low energy indoor positioning. In: IPIN 2014 - 2014 INTERNATIONAL CONFERENCE ON INDOOR POSITIONING AND INDOOR NAVIGATION 2014.

KALBANDHE, Ankush A.; PATIL, Shailaja. C. Indoor Positioning System using Bluetooth Low Energy. In: 2016 INTERNATIONAL CONFERENCE ON COMPUTING, ANALYTICS AND SECURITY TRENDS (CAST) 2016.

LUO, Yi; NANTZ, John. **Vehicle control system to prevent relay attack**, US9963109B2, 2018.

MALAGÓN, Pedro et al. Bitslice software implementation of KeeLoq as a side-channel countermeasure. In: PROCEEDINGS OF THE WESS’15: WORKSHOP ON EMBEDDED SYSTEMS SECURITY - WESS’15 2015, New York, NY, USA. ACM, 2015.

MIYAZAWA, Akira. **Keyless entry apparatus**, US9600948B2, 2017.

OKEYA, Katsuyuki; SAKURAI, Kouichi. On Insecurity of the Side Channel Attack Countermeasure Using Addition-Subtraction Chains under Distinguishability between Addition and Doubling. Information and Security Privacy, p. 420–435, 2002.

PAAR, Christof et al. KeeLoq and side-channel analysis - Evolution of an attack. **Fault**

Diagnosis and Tolerance in Cryptography - Proceedings of the 6th International Workshop, FDTC 2009, [s. l.], p. 65–69, 2009.

POLLITT, Mark M. An ad hoc review of digital forensic models. In: PROCEEDINGS - SADFE 2007: SECOND INTERNATIONAL WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING 2007.

ROBLING DENING, D. E. (1982). **Cryptography and Data Security**. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA

SADOWSKI, Sebastian; SPACHOS, Petros. RSSI-Based Indoor Localization with the Internet of Things. **IEEE Access**, v. 6, p. 30149–30161, 2018.

SCC. **CAN/ULC-S338-98-R2018 - Standard for Automobile Theft Deterrent Equipment and Systems: Electronic Immobilization**.

SEIBERTS, Klaus; CHILDERS, Jim. **Relay attack prevention for passive entry/passive start systems**, US9102296B2, 2015.

SHEETRIT, Idan; WOOL, Avishai. Cryptanalysis of KeeLoq code-hopping using a Single FPGA. **Cryptology ePrint Archive, Report 2011**, v. 2011, n. 242, p. 15, 2011.

SIMMONS, Gustavus J. Symmetric and Asymmetric Encryption. **ACM Computing Surveys**, v. 11, n. 4, p. 305–330, 1979.

SOOS, Mate; NOHL, Karsten; CASTELLUCCIA, Claude. Extending SAT solvers to cryptographic problems. In: LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS), 2009.

ŠTEMBERA, Petr; NOVOTNÝ, Martin. Breaking Hitag2 with reconfigurable hardware. In: PROCEEDINGS - 2011 14TH EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN: ARCHITECTURES, METHODS AND TOOLS, DSD, 2011.

SUN, Siwei et al. Cube cryptanalysis of Hitag2 stream cipher. In: LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS) 2011, Berlin, Heidelberg.

THALJAOUI, Adel et al. BLE localization using RSSI measurements and iRingLA. In: PROCEEDINGS OF THE IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY, 2015.

TILLICH, Stefan; WÓJCIK, Marcin. Security analysis of an open car immobilizer protocol stack. In: LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS), 2012.

TRUONG, Hien Thi Thu et al. Using contextual co-presence to strengthen Zero-Interaction Authentication: Design, integration and usability. In: PERVASIVE AND MOBILE COMPUTING 2015.

VERDULT, Roel; GARCIA, D. Flavio; BALASCH, Josep. Gone in 360 Seconds: Hijacking with Hitag2. **Presented as part of the 21st USENIX Security Symposium**

(USENIX Security 12), p. 237–252, 2012.

VERDULT, Roel; GARCIA, Flavio D. Cryptanalysis of the Megamos Crypto. **USENIX ;login:**, v. 40, n. 6, p. 17–22, 2015.

WANG, Xiaoyun; YU, Hongbo. How to Break MD5 and Other Hash Functions. **Supplement to the 22nd USENIX Security Symposium (USENIX Security 13)**, [s. l.], p. 19–35, 2005.

WANG, Xiaoyun; YU, Hongbo. How to Break MD5 and Other Hash Functions. In: SUPPLEMENT TO THE 22ND USENIX SECURITY SYMPOSIUM (USENIX SECURITY 13) 2005.

WANG, Yankai et al. **Indoor Positioning System Using Euclidean Distance Correction Algorithm with Bluetooth Low Energy Beacon2016 International Conference on Internet of Things and Applications (IOTA)**, 2016.

WELCH, D.; LATHROP, S. Wireless security threat taxonomy. **IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.**, n. June, p. 76–83, 2003.

WOHLIN, Claes. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: **PROCEEDINGS OF THE 18TH INTERNATIONAL CONFERENCE ON EVALUATION AND ASSESSMENT IN SOFTWARE ENGINEERING - EASE '14 2014**.

WOOD, Anthony D.; STANKOVIC, John A. A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. **Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (2004)**, [s. l.], p. 739–763, 2004.

XU, Wenyuan et al. Jamming sensor networks: Attack and defense strategies. **IEEE Network**, [s. l.], v. 20, n. 3, p. 41–47, 2006.

YUAN, Eric; TONG, Jin. Attributed Based Access Control (ABAC) for web services. In: PROCEEDINGS - 2005 IEEE INTERNATIONAL CONFERENCE ON WEB SERVICES, ICWS, 2005.

APÊNDICE A – REVISÃO DE PATENTES

Título	Autor(es)	Proprietário	Identificador	Ano
Access and driver authentication system with increased security against relay attacks using movement sensor technology integrated into the authentication tool	Weghaus Ludger	Hella Kgaa Hueck & Co.	US-9988017-B2	2018
Accessing a vehicle using portable devices	Brian J. Tucker, Emily C. Schubert, Jesse L. Dorogusker, Joakim Linde, Stephen Chick	Apple Inc.	US-8947202-B2	2015
Accessory control with geo-fencing	Sylvain Louboutin	Apple Inc.	US-8868254-B2	2014
Aftermarket sound activated wireless vehicle door unlocker	John Clinton Kolar	John Clinton Kolar	US-8947203-B2	2015
Alternate backup entry for vehicles	Venkatesh Krishnan	Ford Global Technologies, Llc	US-9518408-B1	2016
Anti-theft system for a vehicle, and method for the operation of an anti-theft system	Thomas Georgi, Roland Wagner	Continental Automotive Gmbh	US-8150563-B2	2012
Antitheft system for vehicle	Naoto Yamamoto, Hideaki Arai	Honda Motor Co., Ltd.	US-8299891-B2	2012
Apparatus and method for dual range detection in a vehicle	Stephen Humphrey, Riad Ghabra, Matthew Ryan Honkanen, Ronald O. King	Lear Corporation	US-9902369-B2	2018
Apparatus, system and method for dynamic identification and key management for vehicle access	Heiko Maiwand, Martin Roehder, Payton White, Jaime Camhi	Volkswagen Aktiengesellschaft, Audi Ag	US-9865113-B2	2018
Apparatus, system and method for dynamic identification for vehicle access	Heiko Maiwand, Martin Roehder, Payton White, Jaime Camhi	Volkswagen Aktiengesellschaft, Audi Ag	US-9865112-B2	2018
Apparatus, system and method for vehicle access and function control utilizing a portable device	Heiko Maiwand, Martin Roehder,	Volkswagen Aktiengesellschaft, Audi Ag	US-9870665-B2	2018

	Payton White, Jaime Camhi			
Apparatus, system and method for vehicle access and function control utilizing a portable device	Heiko Maiwand, Martin Roehder, Payton White, Jaime Camhi	Volkswagen Aktiengesellschaft, Audi Ag	US-9902368-B2	2018
Apparatus, system and method for vehicle authentication management and reporting	Dominic WINKELMAN	Volkswagen Ag, Audi Ag	US-9305412-B2	2016
Automatic locking failsafe for vehicles with passive keys	Christopher M. Kurpinski, Thomas J. Keeling, Justin P. McBride, Toshihiro T. Wakamatsu, Michael A. Wiegand	Denso International America, Inc.	US-7683764-B2	2010
Buttonless vehicle key having gesture recognition	Rainer Mittermeier	Bayerische Motoren Werke Aktiengesellschaft	US-9346470-B2	2016
Car control method of electronic apparatus and electronic apparatus thereof	Jeong WOO, Jae Il AN, Jae-young Shin, Sehwan Choi, Hyun-Ju HONG	Samsung Electronics Co., Ltd.	US-10083555-B2	2018
Car management system and method	Hyun-woo Lee	Hyundai Motor Company	US-9911255-B2	2018
Chauffeur function thumbprint lock and ignition systems	David Wooding	David Wooding	US-8892272-B1	2014
Control system and control method for vehicle anti-theft	Chien-Yu Yeh, Po-Hsien Liu	Hon Hai Precision Industry Co., Ltd.	US-9669800-B2	2017
Control system and control method for vehicle anti-theft	Po-Hsien Liu, Yu-Wen Chen	Hon Hau Precision Industry Co., Ltd.	US-9449447-B2	2016
Detection and protection against jam intercept and replay attacks	Allen R. MURRAY, Oliver Lei	Ford Global Technologies, Llc	US-10043329-B2	2018
Distance determination and authentication of a remote control key to a vehicle	Alexander TSCHACHE	Volkswagen Ag	US-9911262-B2	2018

Door courtesy switch abnormality detection apparatus and method	Masachika Kamiya	Toyota Jidosha Kabushiki Kaisha	US-9076274-B2	2015
Door unlocking system	Kazutaka Naitou	Autonetworks Technologies, Ltd., Sumitomo Wiring Systems, Ltd., Sumitomo Electric Industries, Ltd.	US-9783160-B2	2017
Door unlocking system and door unlocking method	Ikuhei KIMURA, Makoto YASUTAKE	Murata Manufacturing Co., Ltd.	US-9997000-B2	2018
Dual purpose wireless device, wherein vehicle controls depend on device location	Michel F. Sultan, Todd P. Oman, Dale L. Partin, Paul J. Ainslie	Delphi Technologies, Inc.	US-8421589-B2	2013
Duplication means for an electronically coded key and related method	David REBULI	Keyline S.P.A.	US-8750510-B2	2014
Electronic communication module for locking/unlocking a movable panel of a motor vehicle, associated control central processing unit, and hands-free access system	Eric Leconte	Valeo Securite Habitacle	US-9996994-B2	2018
Electronic key system	Carlos TERCERO	Denso Corporation	US-9919679-B2	2018
Gesture controls for remote vehicle access systems	Robert J. Campbell, Yipeng Tang, Mansour Ashtiani, Khalid Kamal, Lynn D Da Deppo	Huf North America Automotive Parts Manufacturing, Corp.	US-9646436-B1	2017
Hands free access system for a vehicle closure	Rini Sherony	Toyota Motor Engineering & Manufacturing North America, Inc.	US-9598049-B2	2017

ID-based control unit-key fob pairing	Jin-Meng Ho, Eric Peeters	Texas Instruments Incorporated	US-9516500-B2	2016
In-vehicle device controller	Kazuhiro Nakashima, Arinobu Kimura, Hiroki Okada, Hiroko Murakami	Denso Corporation, Toyota Jidosha Kabushiki Kaisha	US-8860550-B2	2014
Integrated immobilizer fob pairing	Emmanuel Enrique Lopez	Secured Mobility, Llc	US-9454860-B2	2016
Intelligent access system and method for a vehicle	Vivek Jain, Maurizio Bocca, Huang Lee, Christoph Lang, Abtin Keshavarzian	Robert Bosch Gmbh	US-10083556-B1	2018
Intermediary access device for communication with a vehicle	Hans-Peter Fischer, Timothy Barrett, Andreas KASPRZOK, Keith Payne, Johannes Michael ZAHN	Bayerische Motoren Werke Akttiengesell schaft	US-10062223-B2	2018
Key fob challenge request masking base station	John Robert Van Wiemeersch, Joey Ray Grover, Scott Smereka, Justin Dickow	Livio, Inc.	US-9940764-B2	2018
Key fob security copy to a mobile phone	David Anthony Hatton	Ford Global Technologies, Llc	US-9002536-B2	2015
Keyfob proximity theft notification	Christopher L. Oesterling	GM Global Technology Operations LLC	US-8638202-B2	2014
Keyless entry apparatus	Akira Miyazawa	Alps Electric Co., Ltd.	US-9600948-B2	2017
Keyless entry device	Akira Miyazawa	Alps Electric Co., Ltd.	US-9342938-B2	2016
Keyless entry device	Akira Miyazawa	Alps Electric Co., Ltd.	US-9849860-B2	2017
Keyless entry device of vehicle	Yoshio Sampei	Alps Electric Co., Ltd.	US-8400262-B2	2013
Keyless entry system	Akira Miyazawa	Alps Electric Co., Ltd.	US-9260079-B2	2016

Keyless entry system	Junya YASUI, Akira Miyazawa	Alps Electric Co., Ltd	US-9424698-B2	2016
Keyless entry system	Katsuhiro SEINO	Alps Electric Co., Ltd.	US-9378603-B2	2016
Keyless entry system	Satoshi Nakajima, Satoshi Hayasaka	Alps Electric Co., Ltd.	US-8044771-B2	2011
Keyless entry system	Yuuto Kameyama, Tomoyuki Funayama, Shoji Kakinuma	Denso Corporation, Toyota Jidosha Kabushiki Kaisha	US-9299205-B2	2016
Keyless entry system and vehicle-mounted device	Akira Miyazawa	Alps Electric Co., Ltd.	US-9919680-B2	2018
Keyless vehicle systems	Venkatesh Krishnan	Ford Global Technologies, Llc	US-9725069-B2	2017
Lock control method requiring activation by a first channel and authorization by a second different channel	Justin Wang	Leadot Innovation, Inc.	US-9697662-B2	2017
Lock-unlock system for vehicle	Shigeki Nishiyama, Tomoyuki Funayama	Toyota Jidosha Kabushiki Kaisha	US-9672675-B1	2017
Low latency inside/outside determination for portable transmitter	Riad Ghabra, Nikolay Yakovenko, Hilton W. Girard	Lear Corporation	US-8427289-B2	2013
Memory management for fleet operation of PEPS vehicles	David T. Proefke, Ron Y. Asmar, Thomas E. Utter, Aaron P. Creguer	GM Global Technology Operations LLC	US-9728018-B2	2017
Method and apparatus for digital temporary vehicle key utilization	Vijayababu Jayaraman, Ali Mohamad Suleiman, Karl Nathan Clark, Mohamad Nasser, John Naum Vangelov	Ford Global Technologies, Llc	US-9688247-B1	2017
Method and apparatus for implementing multi-vendor rolling code keyless entry systems	Daniel Charles Johnson, Michael Calvin	Ikeyless, Llc	US-10115255-B2	2018

	McCoy, Daniel Patrick Bowen			
Method and apparatus for providing vehicle security	Jason Aurele Soroko	Entrust, Inc.	US-9767627-B2	2017
Method and device for managing access control	Johannes Ullmann	Evva Sicherheitstechnologie Gmbh	US-8635462-B2	2014
Method and system for a key fob base station enabling remote car access using a nomadic device	Jacob R. Sigal, Joey Ray Grover, Michael Burke, Scott Smereka, Joel J. Fischer	Livio, Inc.	US-9754431-B2	2017
Method and system for access control	Jorge Clemente, Thomas Schlechter, Reinhard Surkau	Skidata Ag	US-9715773-B2	2017
Method and system for authenticating vehicle equipped with passive keyless system	Ron Y. Asmar, David T. Proefke, Charles J. Bongiorno, Aaron P. Creguer	GM Global Technology Operations LLC	US-9710983-B2	2017
Method and system for detecting proximity of an end device to a vehicle based on signal strength information received over a bluetooth low energy (BLE) advertising channel	Neeraj R. Gautama, Amanda J. Kalhous, Robert A. Hrabak, Norman J. Weigert	GM Global Technology Operations LLC	US-9008917-B2	2015
Method and system for remote access control	Nikolas Bergerhoff, Ritesh Ahuja, Adrian Radu, Tejas Desai, Herbert Froitzheim, Yao Zhai, Robert Obermaier	Continental Intelligent Transportation Systems, LLC	US-9852563-B2	2017
Method and system for secure and authorized communication between a vehicle and wireless communication devices or key fobs	Neeraj R. Gautama, Amanda J. Kalhous, Shaun S. Marshall,	GM Global Technology Operations LLC	US-9218700-B2	2015

	Kenneth L. Peirce			
Method for controlling a door of a vehicle	Stefan Hermann	Continental Automotive Gmbh	US-8935052-B2	2015
Method for determining the location of a remote transmitter positioned near a vehicle	Daniel Kornek, Ewen James Christopher	Robert Bosch (Australia) Pty Ltd	US-9694787-B2	2017
Method for operating an authorization device for a keyless access to and start of a vehicle	Ingo Ledendecker	Audi Ag	US-9002540-B2	2015
Method for performing authentication and electronic device thereof	Moon-Su CHANG, Yang-Soo Lee, Joo-Yeon Lee, Dong-Hyun YEOM	Samsung Electronics Co., Ltd.	US-9865107-B2	2018
Method for processing a presence signal in a hands-free vehicle access system having capacitive sensors	Bachir Ayeva, Thierry BELLEZA, Isabelle VERDON	Continental Automotive France, Continental Automotive Gmbh	US-9406179-B2	2016
Method for protecting a hands-free access and/or starting system of a vehicle by modifying the speed of signal reception	Alain Brillon, Isabelle VERDON	Continental Automotive France, Continental Automotive Gmbh	US-9430889-B2	2016
Method of automatically unlocking an opening member of a motor vehicle for a hands-free system, and device for implementing the method	Frederic Giraud, Eric Menard, Joel Senpauroca	Valeo Securite Habitacle	US-8717429-B2	2014
Method to facilitate communication between a lock and a key	Zubair Mohammad, John Draper, Stefan Ferber	Robert Bosch Gmbh	US-10055920-B2	2018
Method, system, and computer program product for establishing a temporary remote control association between a mobile device and a peripheral device	James Mills, Mario Sorce, David Wong	Kaba Ilco Inc.	US-9922480-B2	2018
Method, system, and computer-readable medium relating to internet of things-enabled remote controls	Kyu Han Chong	Kyu Han Chong	US-9779571-B2	2017
Mobile control node system and method for vehicles	Hasib HASSAN, Devendra	Magna Electronics, Inc.	US-8373581-B2	2013

	Bajpai, Uri Levy			
Mobile device and key fob pairing for multi-factor security	Steven Birkel, Rita Wouhaybi, Tobias Kohlenberg, Stanley Mo, Joni D. Stutman	Intel Corporation	US-8933778-B2	2015
Mobile device for vehicle	Satoshi Nakajima, Satoshi Hayasaka, Masaki Sato, Jun Takahashi	Alps Electric Co., Ltd.	US-8232863-B2	2012
Mobile identification transmitter which can be set to a normal state and a secure state	Alexander Geldmacher	Huf Hulsbeck & Furst Gmbh & Co. Kg	US-8972078-B2	2015
Movement history assurance for secure passive keyless entry and start systems	Zoran Zivkovic, Jan René Brands, Frank Harald Erich Ho Chung LEONG, Stefan Drude	Nxp B.V.	US-8976005-B2	2015
Movement pattern detection in a vehicle communication system	Howard Siswick, Mohammed Khan	Jaguar Land Rover Limited	US-9969356-B2	2018
NFC based secure car key	Bernhard Spiess, Ulrich Neffe	Nxp B.V.	US-9786108-B2	2017
On-vehicle apparatus control system and on-vehicle control device	Masahiro Yamamoto, Yoichi Atsumi	Omron Automotive Electronics Co., Ltd.	US-9786110-B2	2017
On-vehicle apparatus control system, on-vehicle control device, and portable machine	Masahiro Yamamoto, Yoichi Atsumi	Omron Automotive Electronics Co., Ltd.	US-9965912-B2	2018
On-vehicle apparatus, vehicle locking/unlocking system, and method of controlling on-vehicle apparatus	Shigeki Nishiyama, Tomoyuki Funayama, Toru Yoshihara	Toyota Jidosha Kabushiki Kaisha	US-9792745-B2	2017
Outboard motor antitheft apparatus	Masato Takeda, Yoshihisa Shinogi, Masashi MANITA, Kosei	Honda Motor Co., Ltd.	US-8357018-B2	2013

	Yamashita, Makoto Yamamura, Yoshinori Maekawa			
Passive entry cell phone and method and system therefor	Joseph Santavicca	Voxx International Corporation	US-9241235-B2	2016
Passive entry system and method for a vehicle	Riad Ghabra	Lear Corporation	US-9129454-B2	2015
Passive entry system for an automotive vehicle	Riad Ghabra, Ehab Abdulla Tarmoom	Lear Corporation	US-8531268-B2	2013
Passive remote keyless entry system with time-based anti-theft feature	Xing Ping Lin	Trw Automotive U.S. Llc	US-9842445-B2	2017
Phone sleeve vehicle fob	John Robert Van Wiemeersch, Robert Bruce Kleve, Kevin Thomas Hille	Ford Global Technologies, Llc	US-9842444-B2	2017
Portable device, communication device, and communication system	Kazuya Hamada, Takahiro Inaguma, Yosuke TOMITA	Omron Automotive Electronics Co., Ltd.	US-9728025-B2	2017
Position-based performance of a vehicle function in a vehicle communication system	Howard Siswick, Mohammed Khan	Jaguar Land Rover Limited	US-9764699-B2	2017
Priming vehicle access based on wireless key velocity	Arthur Thomas Bianchi, III, Kevin F. Militello, John Robert Van Wiemeersch, Vivekanandh Elangovan	Ford Global Technologies, Llc	US-9886805-B1	2018
Provision of a status indication to a user in a vehicle communication system	Howard Siswick, Mohammed Khan	Jaguar Land Rover Limited	US-9764713-B2	2017
Proximity confirming passive access system for vehicle	Michael J. Melaragni, William A. Biondo, David T. Proefke	GM Global Technology Operations LLC	US-9855918-B1	2018
Regulating vehicle access using cryptographic methods	Karl B. Leboeuf, Ramie Phillips,	GM Global Technology	US-9990783-B2	2018

	Iii, Earnest A. Lucitte, III	Operations LLC		
Relay attack inhibiting	Bjorn Markus Jakobsson	Qualcomm Incorporated	US-9802574-B2	2017
Relay attack prevention for passive entry passive start (PEPS) vehicle security systems	Todd P. Oman, Kevin J. Hawes	Delphi Technologies, Inc.	US-8930045-B2	2015
Relay attack prevention for passive entry/passive start systems	Klaus Seiberts, Jim Childers	Texas Instruments Incorporated	US-9102296-B2	2015
Remote control button actuation module, system, and method	Craig Arnold Tieman	Tieman Vehicle Technologies LLC	US-9576414-B2	2017
Remote control device, vehicle, and method for controlling the vehicle	Jihye Lee, Jongyoung LEE, Sinjung Kim	Hyundai Motor Company	US-10078932-B2	2018
Remote control system for car-mounted device	Yoshitsugu Sawa, Hiroshi Araki, Yukio Goto, Masashi Nojima, Masanobu Hiramine	Mitsubishi Electric Corporation	US-8228164-B2	2012
Remote control system using different types of carrier waves for polling signals	Riad Ghabra	Lear Corporation	US-9685014-B1	2017
Remote identification device associated with a vehicle including means for remotely communicating battery state-of-charge information with the associated vehicle	Eric Menard	Valeo Securite Habitacle	US-8912912-B2	2014
Remote keyless system	Thomas Zane Pramudji, Ari Pramudji	Thomas Zane Pramudji, Ari Pramudji	US-9767633-B2	2017
Remote management and control of vehicular functions via multiple networks	Lonny Baskin, Ariel Malamud	Intel Corporation	US-9031712-B2	2015
Remote vehicle access system	Eric E. HELLIGRATH	Honda Motor Co., Ltd.	US-10055916-B1	2018
Remote vehicle access systems for fleet vehicles	Leonardo POMA	Huf North America Automotive Parts Manufacturing Corp.	US-9896063-B2	2018
Reuseable keyfob for use prior to sale of keyless vehicle	Venkatesh Krishnan	Ford Global Technologies, Llc	US-9607457-B2	2017

RFID transponder and method for operating the same	Ernst Muellner, Carlo Peschke	Texas Instruments Deutschland Gmbh	US-8923791-B2	2014
Security system for a motor vehicle	Carl Anthony Pickering	Jaguar Cars Limited	US-7710245-B2	2010
Smart entry system	Hiroki Inoue	Denso Corporation	US-10008060-B2	2018
Smart entry system	Katsuyasu Yamane, Masayuki Yamazaki	Honda Motor Co., Ltd.	US-9607460-B2	2017
Smart entry system	Katsuyasu Yamane, Shinichi Arie, Masayuki Yamazaki	Honda Motor Co., Ltd.	US-9396597-B2	2016
Smart key system	Toru Yoshihara	Toyota Jidosha Kabushiki Kaisha	US-9761075-B2	2017
Smart key system	Yoshiaki Takeuchi, Takeshi Konno, Katsuhisa Yamada, Sadanori Watarai, Kazuyuki Kuriyama, Shuichi ISHIBASHI	Honda Motor Co., Ltd., Honda Lock Mfg. Co., Ltd.	US-8423203-B2	2013
Smart keyless entry system	Yasushi Hamada	Mazda Motor Corporation	US-8310338-B2	2012
Solutions for relay attacks on passive keyless entry and go	Carlo Secondo Mutti, Davide Spedaliere	Assa Abloy Czech & Slovakia S.R.O.	US-9349236-B2	2016
System allowing a service provider to selectively open a vehicle	Joris Fokkelman	Continental Automotive Gmbh	US-9652908-B2	2017
System and method for activating and deactivating a remotely controlled vehicle starter	Jose L. Gallarzo	Gallarzo Jose L	US-8354919-B2	2013
System and method for authenticating components of a vehicle	Mukesh B. Nair	Nxp B.V.	US-9685013-B2	2017
System and method for authorizing a remote device	Hilton W. Girard, III, Nikolay	Lear Corporation	US-8344850-B2	2013

	Yakovenko, Riad Ghabra			
System and method for communicating with a vehicle	Craig A. Tieman	Samsung Electronics Co., Ltd.	US-8847731-B2	2014
System and method for controlling vehicle systems from a cell phone	Jamie C. Howarter, Richard G. Bradford	Centurylink Intellectual Property Llc	US-8224313-B2	2012
System and method for factory key code display with an automotive keyless entry system	Ronald Patrick Brombach, Mark Christian Aaron, Lisa Therese Boran, Daniel James Card	Ford Global Technologies, Llc	US-8154383-B2	2012
System and method for key free access to a vehicle	Jamie C. Howarter, Richard G. Bradford	Embarq Holdings Company Llc	US-8126450-B2	2012
System and method for keyless entry and remote starting vehicle with an OEM remote embedded in vehicle	Jack Wisnia	Lightwave Technology Inc.	US-9536365-B2	2017
System and method for operating vehicle using mobile device	Phillip John Weicker, Anil Paryani	Faraday & Future Inc.	US-9830757-B2	2017
System and method for range-boosted key fob	II Charles Everett Badger	Ford Global Technologies, Llc	US-9842447-B2	2017
System and method for training a programmable transceiver	Todd R. Witkowski, Ivo Ivanov Bonev, Plamen Chavdarov Stoyanov, Stefan Rumenov Nikolov	Gentex Corporation	US-10008109-B2	2018
System and method to enable passive entry	Timothy K. Mitchell	Fca Us Llc	US-9129455-B2	2015
System for assigning a smartphone as a temporary key for a vehicle	John Avery, Adeel Yusuf	Panasonic Automotive Systems Company Of America, Division Of Panasonic Corporation Of North America	US-9595145-B2	2017

System for passive entry and passive start for a motor vehicle	Danilo Caratto, Carlo Piazano, Samuele Ginevro	TRW Automotive Italia SRL	US-9045102B2	2015
System including a hand-held communication device having a motion sensor for remotely controlling the position of a door of a land vehicle and key fob for use in the system	Jason T. Murar, Darius J. Preisler, David R. Syrowik	Jvis-Usa, Llc	US-9593522-B1	2017
System including a hand-held communication device having low and high power settings for remotely controlling the position of a door of a land vehicle and key fob for use in the system	Jason T. Murar, Darius J. Preisler, David R. Syrowik	Jvis-Usa, Llc	US-9830755-B2	2017
Time of flight based passive entry/passive start system	Kobi J. Scheim, Moshe Laifenfeld, Nadav Lavi	GM Global Technology Operations LLC	US-9894613-B2	2018
Upgrade kit for an ignition key and methods	John Stanfield, Eric D. Aeby, Michael Javault, Clement Gires, Brian Ng	Local Motion, Inc.	US-8841987-B1	2014
Vehicle access authentication	Pietro Buttolo, II James Stewart Rankin, Mengchi Wang, Stuart C. Salter	Ford Global Technologies, Llc	US-9875589-B1	2018
Vehicle access system	Mohammed Khan, Howard Siswick	Jaguar Land Rover Limited	US-9563990-B2	2017
Vehicle and control method thereof	Jongyoung LEE, Jihye Lee, Sinjung Kim	Hyundai Motor Company	US-9783161-B2	2017
Vehicle communication status indicator	Rafic Jergess, John Robert Van Wiemeersch, Howard Paul Tsvi Linden	Ford Global Technologies, Llc	US-9922472-B2	2018
Vehicle control apparatus	Tomoyuki Funayama	Toyota Jidosha Kabushiki Kaisha	US-9569903-B2	2017

Vehicle control apparatus	Yosuke TOMITA, Naoyuki Ishihara, Tetsuo Nishidai, Takahiro Inaguma, Kazuya Hamada	Omron Automotive Electronics Co., Ltd.	US-9710985-B2	2017
Vehicle control system to prevent relay attack	Yi Luo, John Nantz	Huf North America Automotive Parts Mfg. Corp.	US-9963109-B2	2018
Vehicle door control	Robert Bingle, C. Bruce Banter	Adac Plastics, Inc.	US-9696839-B1	2017
Vehicle electronic key system	Chia-Wei Chang, Shiang-Hua Lin, Ping-Mao Lee, Kuang-Yao Liao, Chih-Chung Weng, Hsin-Nan Chen	Hon Hai Precision Industry Co., Ltd.	US-9536360-B2	2017
Vehicle function restriction system	Hiroshi Tsuruta, Kenji Suzuki	Kabushiki Kaisha Tokai Rika Denki Seisakusho	US-8487740-B2	2013
Vehicle immobilizing devices, systems, and methods	Gregory S. Hopper, Peter Kent McCammon, Neal Harris Stern, Elizabeth Wells Shumadine	Pra Group, Inc.	US-9156436-B2	2015
Vehicle key function control from a mobile phone based on radio frequency link from phone to vehicle	Robin D. Katzer	Sprint Communications Company L.P.	US-9252951-B1	2016
Vehicle keyless operation system and method	Brian K. Lickfelt, Hideaki Arai, Jason D. DiSalvo	Honda Motor Co., Ltd.	US-8249802-B2	2012
Vehicle lock-out protection system	Brian Karl LICKFELT, Bharath Kumar	Honda Motor Co., Ltd.	US-9976322-B2	2018

	PARASURAMA			
Vehicle PEPS system using directional sensors	Vyacheslav Berezin, Shaun S. Marshall, Moshe Laifenfeld, Timothy J. Talty	GM Global Technology Operations LLC	US-9928673-B2	2018
Vehicle remote function system and method for determining vehicle FOB locations using adaptive filtering	Thomas O'Brien, Jason G. Bauman, Jian Ye	Lear Corporation	US-9679430-B2	2017
Vehicle remote function system and method for effectuating vehicle operations based on vehicle FOB movement	Jason G. Bauman, Thomas O'Brien, Jian Ye	Lear Corporation	US-9852560-B2	2017
Vehicle security system	Riccardo MORSELLI	Cnh Industrial America Llc	US-9865108-B2	2018
Vehicle system and method for keyless authentication and control of an ignition system	Julianne KRAWCIW	Denso International America, Inc., Denso Corporation	US-9862353-B2	2018
Vehicle wireless communication system, vehicle control device, and portable machine	Kazuya Hamada, Takahiro Inaguma, Yosuke TOMITA	Omron Automotive Electronics Co., Ltd.	US-9646443-B2	2017
Vehicle wireless communication system, vehicle control device, and portable machine	Kazuya Hamada, Takahiro Inaguma, Yosuke TOMITA, Tetsuo Nishidai, Yuki Tokuyama	Omron Automotive Electronics Co., Ltd.	US-9805532-B2	2017
Vehicular security system with configurable immobilization features	David S. Magner, Anita L. Reichling	Trimark Corporation	US-8976014-B2	2015
Wireless communication system for vehicle	Masanori Kosugi	Kabushiki Kaisha Tokai Rika Denki Seisakusho	US-9070232-B2	2015
Wireless communications circuit	Frank Leong, Jan Van Sinderen,	Nxp B.V.	US-9082241-B2	2015

	William Redman-White			