Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Arthur Fernandes Miler Amoroso

Leonardo Magalhães Redondo

SEGURANÇA DA INFORMAÇÃO EM IOT E CARROS AUTÔNOMOS

Americana, SP

2020

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Arthur Fernandes Miler Amoroso

Leonardo Magalhães Redondo

SEGURANÇA DA INFORMAÇÃO EM IOT E CARROS AUTÔNOMOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. João Emmanuel D´Alkmin Neves.

Área de concentração: Segurança da Informação.

Americana, SP.

2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

A547s AMOROSO, Arthur Fernandes Miler;

Segurança da informação em IoT e carros autônomos. / Arthur Fernandes Miler Amoroso; Leonardo Magalhães Redondo. – Americana, 2020.

37f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. João Emmanuel D' Alkmin Neves

1 Internet das coisas 2. Carros autônomos 3. Segurança em sistemas de informação I. REDONDO, Leonardo Magalhães II. NEVES, João Emmanuel D' Alkmin II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Arthur Fernandes Miler Amoroso

Leonardo Magalhães Redondo

SEGURANÇA DA INFORMAÇÃO EM IOT E CARROS AUTÔNOMOS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 30 de junho de 2020.

Banca Examinadora:

_____
Professor João Emmanuel D' Alkmin Neves
Mestre
Fatec Americana

_____
Professor Adriano Cilhos Doimo
Especialista
Fatec Americana

_____
Professor Maxwel Vitorino da Silva
Mestre
Fatec Americana

AGRADECIMENTOS

Toda obra antes de ser concluída percorre por uma jornada de desafios e superações, e em meio aos desafios que encontramos forças para enfrentar e superar os obstáculos.

Em primeiro lugar, agradecemos á todos os indivíduos que participaram diretamente do desenvolvimento desse trabalho, mantendo a harmonia e apoio mútuo para que os fundamentos fossem organizados entre linhas e concluindo um trabalho de responsabilidade com a informação.

Em segunda mão, agradecemos diretamente as pessoas que acompanharam o desenvolvimento deste projeto, as quais contribuíram com sugestões e críticas construtivas. Dentre essas, professores que sempre presentes, ajudaram em dúvidas que surgiam durante a desenvoltura como a professora Maria Cristina Aranda, e o nosso orientador de TCC , que auxiliou na comprovação de dados verídicos e pesquisas científicas realizadas nos últimos anos.

E por último, e não menos importante, agradecemos aos nossos familiares que sempre apoiaram em nossas decisões, juntamente com a nossa querida instituição de ensino Faculdade de Tecnologia de Americana, que nos deu a oportunidade de aprendizado durante esses anos de ensino. E todo o corpo docente que por trás desse nome, trabalham duramente para fazer acontecer - em especial nosso Diretor Rogério Freitas.

Nossos sinceros agradecimentos.

DEDICATÓRIA

Dedicamos este trabalho a todos os professores do curso, que foram de extrema importância ao decorrer dos anos letivos transmitindo seus conhecimentos e dando suporte. Aos amigos de sala, pelas alegrias, tristezas e todos os outros momentos compartilhados. E familiares, pelo incentivo e pelo apoio constante. A todos os futuros estudantes da instituição.

RESUMO

Carros autônomos, foram apresentados em literatura desde 1920 (Ricardo Caruso, 2017), nessa época já se falava sobre carros que possuíam alguma autonomia, como um Houdina Radio Control.

Atualmente chegamos ao estado da arte quando o assunto é carros inteligentes, pois nessa configuração eles apresentam inúmeros sensores, sistema embarcado e a internet (IoT).

A IoT (Internet das coisas), deixou de ser apenas um conceito, para se tornar realidade em nossas vidas, com o avanço da tecnologia, cada vez mais podemos notar dispositivos do cotidiano agindo de forma inteligente e automatizando nossas tarefas.

O intuito da IoT é interligar esses dispositivos a rede para obtermos um controle melhor e mais eficiente e abordar nichos como o setor automotivo, desenvolvendo tecnologias para aproximar cada vez mais a percepção humana.

A principal ideia de fazer carros autônomos foi para diminuir os riscos humanos em acidentes, já que em teoria todos os carros estariam conectados a uma rede de comunicação entre si e seus serviços. Podendo identificar ruas/rodovias lotadas e tentar evitá-las, acidentes seriam reduzidos de mortes para feridos medianamente, além de não ser mais necessário um motorista.

Atualmente, onde tudo pode se conectar a internet pode virar uma faca de dois gumes, onde por um lado tudo fica mais fácil de obter e de levar consigo, por outro lado, criminosos cibernéticos podem estar a espreita, esperando alguém fazer algum erro para possivelmente obter informações da pessoa alvo. Com este problema em mãos, a segurança dos veículos autônomos está sendo posta em testes, onde Hackers, White Hats e Grey Hats, tentam de alguma forma acessar o veículo e mostrar que é possível o risco de vida humana se não for totalmente protegido.

Casos como: veículos autônomos em acidentes de trânsitos podem ser facilmente achados pela internet, onde em sua maioria são outros carros que tendem a bater no veículo, porém em um dos casos aconteceu de um veículo autônomo colidir com um caminhão, acidentes como este é importante para obter dados e para tentar superar os obstáculos deste projeto visionário e ambicioso.

Palavras Chave: IoT, Carros Autônomos, Segurança da Informação em Veículos.

ABSTRACT

Autonomous cars have been presented in literature since 1920 (Ricardo Caruso, 2017), at that time people were talking about cars that had some autonomy, like a Houdina Radio Control.

Currently we have reached the state of the art when it comes to smart cars, because in this configuration they have numerous sensors, embedded system and the internet (IoT).

The IoT (Internet of things), has ceased to be just a concept, to become reality in our lives, with the advancement of technology, we can increasingly notice everyday devices acting intelligently and automating our tasks.

The purpose of the IoT is to connect these devices to the network to obtain better and more efficient control and to address niches such as the automotive sector, developing technologies to bring human perception closer and closer.

The main idea of making autonomous cars was to reduce human risks in accidents, since in theory all cars would be connected to a communication network between themselves and their services. By being able to identify crowded streets / highways and try to avoid them, accidents would be reduced from deaths to injuries injured on average, in addition to no longer needing a driver.

Currently, where everything can connect to the internet it can become a double-edged sword, where on the one hand everything is easier to obtain and take with you, on the other hand, cyber criminals may be lurking, waiting for someone to make a mistake to possibly get information from the target person. With this problem in hand, the safety of autonomous vehicles is being put to the test, where Hackers, White Hats and Gray Hats, try to somehow access the vehicle and show that the risk of human life is possible if it is not fully protected.

Cases such as: autonomous vehicles in traffic accidents can be easily found on the internet, where most of them are other cars that tend to hit the vehicle, however in one case an autonomous vehicle collided with a truck, accidents like this are important to obtain data and to try to overcome the obstacles of this visionary and ambitious project.

***Keywords**: IoT, Autonomous Cars, Vehicle Information Security.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SIGLAS

Sigla 1: IoT – (Internet of Things) Internet das Coisas

Sigla 2: VA – Veículos Autônomos

Sigla 3: IBM - International Business Machines

Sigla 4: ITU - International Telecommunication Union

Sigla 5: SO – Sistema Operacional

Sigla 6: ECU - Controller Area Network

Sigla 7 LG - Lucky Goldstar

Sigla 8: BMW - Bayerische Motoren Werke

Sigla 9: MIT - Massachusetts Institute of Technology

Sigla 10: RFID - Radio Frequency Identification

Sigla 12: TV – Televisão

Sigla 13: GM - General Motors

Sigla 14: VaMP - Versuchsfahrzeug für autonome Mobilität und Rechnersehen

Sigla 15: CAN - Controller Area Network

Sigla 16: ABI - Association of British Insurers

1 INTRODUÇÃO

O presente trabalho, aborda uma linha de raciocínio a respeito da evolução da Internet das Coisas e sua aplicação em carros autônomos. O desenvolvimento desta tecnologia, abre portas para a necessidade de formalizar alguns problemas nos quais podem surgir durante os próximos anos, tais como: O quão seguro o carro autônomo será contra hackers? Como o consumidor irá agir com possíveis acidentes originados por erros na programação do carro? Como será a aplicação desses carros em ruas estreitas e mal estruturadas, dê exemplos no Brasil? O quanto de dados sobre o dono do veículo poderá ser gerado e quais comportamentos dessas pessoas as empresas responsáveis poderão adquirir?

Os casos estudados neste documento, que pode-se observar um a um, apontam para a importância de ter um estudo aprofundado sobre as questões acima levantadas, no qual podemos dizer que certas problematizações com carros autônomos estão próximas da realidade.

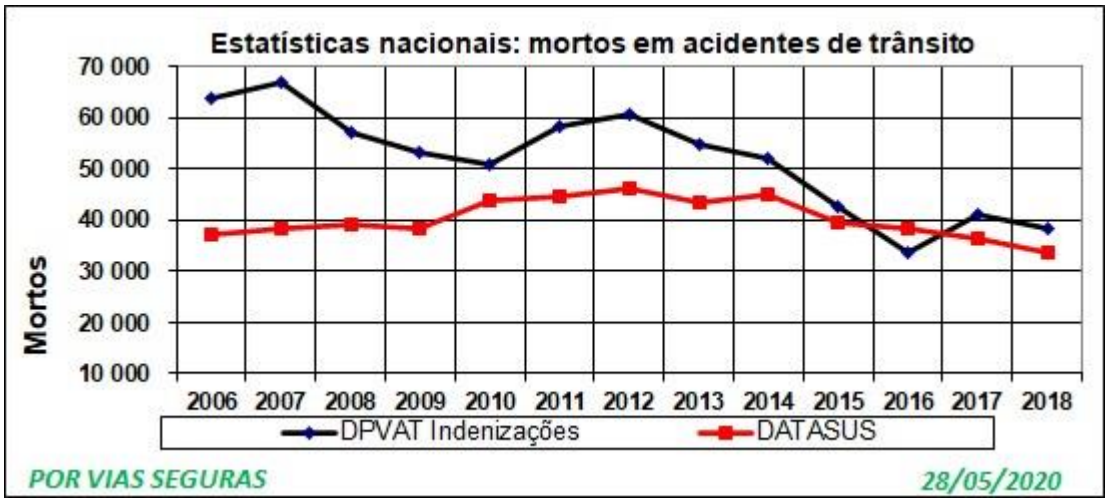
Casos de quebra de dados sigilosos, facilidade de invasão a softwares, controle indevido dos carros por terceiros, acidentes decorrentes de decisões não humanas e também uma enorme quantia de dados gerados a respeito de sua localização em tempo real, tempo que passa no trânsito, o quanto de combustível gasta por dia, informações sobre sua rotina e muito mais. O estudo tem a intenção de abrir uma nova perspectiva a respeito da segurança desses dados e o seu uso indevido.

A nossa experiência histórica na evolução da informática construiu uma bagagem de informações boas e ruins que ficaram registradas durante esse tempo, que permitiu aprender os devidos cuidados contra ações de pessoas com intenções duvidosas na internet, tais como: golpes online, clonagem de cartões de crédito, dados pessoais, roubos de e-mails e senhas entre outros.

O objetivo dessa pesquisa é ajudar a inibir más ações que poderão utilizar a tecnologia desenvolvida em carros autônomos para expandir as más ações que são frequentes na internet. É ajudar a compreender quais as vantagens e desvantagens que poderão surgir durante o tempo, quais decisões poderão ser tomadas pelo computador em decidir em casos extremos qual vida salvar, ou até mesmo relatar testes realizados em ocasiões não frequentes.

A maior motivação para a criação de um veículo autônomo foi para diminuir acidentes em trânsito, quantidades absurdas de acidentes que poderiam ser evitados facilmente são catalogadas todos os anos em vários países. Mesmo que não haja a morte, os feridos de forma grave podem ser possivelmente invalidados de trabalhar. As figuras abaixo mostram o quanto diminuiu as mortes, e o quanto aumentou os feridos graves ao longo dos anos.

Figura 1 Estatísticas nacionais de mortos em acidentes de trânsito



Fonte: Vias Seguras (2020)

Figura 2 Estatísticas nacionais de feridos graves em acidentes de trânsito

Fonte: Vias Seguras (2020)

2 IOT (INTERNET OF THINGS - INTERNET DAS COISAS)

A Internet ajudou as pessoas a se conectarem em um mundo digital vasto de informações disponíveis que é o que conhecemos hoje, mas agora está ajudando a criar conexões de pessoas para pessoas, pessoas para objetos físicos e objetos para outros objetos físicos. A IBM estima que 90% de todos os dados gerados pelos dispositivos como tablets e smartphones etc. nunca são analisados.

Até 60% desses dados começam a perder valor dentro de milissegundos de geração. Conforme estimativas do relatório da IDC, haverá 30 bilhões de Dispositivos conectados à Internet e habilitados para sensores até 2020. No entanto, mais de 99% dos objetos no ambiente físico o mundo ainda permanece desconectado. O rápido crescimento e convergência de dados e processos da Internet está tornando conexões em rede mais relevantes e valiosas.

Você vai receber alguém para jantar. Enquanto dirige do trabalho para casa, com o carro dizendo qual a rota menos congestionada, sua aspirador de pó limpa a sala e seu fogão se prepara para cozinhar uma boa refeição. Mudou de ideia? A televisão escolhe a melhor programação e o telefone faz seu pedido de comida chinesa. Essa é a visão da Ericsson de uma web social das coisas, mostrada em um vídeo que apresenta o protótipo de uma casa não só conectada e inteligente, mas também muito simpática e preocupada com seu dono.

2.1 IoT - Linha do tempo

O termo “internet das coisas”, é mencionado pela primeira vez em 2001 no livro branco de Brock, também pesquisador do Auto-ID Center (BROCK, 2001). Entretanto, Kevin Ashton, outro pesquisador do Auto-ID Center, reclama para si a paternidade do termo. Ashton diz que em 1999, usou a expressão pela primeira vez enquanto falava sobre as potencialidades do RFID na cadeia de abastecimento da multinacional Procter & Gamble. (ASHTON, 2009; UCKELMANN et al, 2011). Naquele momento, ele falava de uma internet das coisas para chamar a atenção dos empresários para o fato de que existem coisas que computadores fazem melhor do que as pessoas que têm tempo, atenção e precisão limitadas.

Outro possível nascimento do termo foi no ano de 1999, quando o então diretor do consórcio de pesquisa “Things that Think” do MIT Media Lab, Neil Gershenfeld,

publicou “When Things Start to Think” (1999). O livro prevê e descreve algumas experiências de computação usável, nanotecnologia e preocupações relacionadas às emoções e direitos civis em uma realidade onde objetos processam informação.

Logo depois, aparece o primeiro eletrodoméstico ‘inteligente’: em junho de 2000, a LG apresentou sua geladeira inteligente durante um evento na Coreia do Sul11. O produto deveria fazer par com outros dispositivos, todos conectados à Internet e gerenciáveis através de um sistema da própria LG.

Na ocasião, o presidente da LG nos Estados Unidos, Simon Kang disse que o eletrodoméstico não apenas resfriava os alimentos como "Consumers can use the Internet refrigerator as a TV, rádio, Web appliance, videophone, bulletin board, calendar and digital camera"

Foi então em 2005 que a discussão sobre a IoT se generalizou, começou a ganhar a atenção dos governos e aparecer relacionada a questões de privacidade e segurança de dados. Foi neste ano que a Internet das Coisas se tornou a pauta do International Telecommunication Union (ITU), agência das Nações Unidas para as tecnologias da informação e da comunicação, que publica anualmente um relatório sobre tecnologias emergentes.

Em 2008, foi publicado The Internet of Things de Rob Van Kranenburg, que busca falar sobre um novo paradigma no qual objetos produzem informação e é uma das grandes referências teóricas sobre a IoT. No mesmo ano aconteceu a primeira Internet of Things Conference em Zurique na Suíça, evento que teve suas discussões compiladas em um livro publicado no mesmo ano sob a organização de Christian Floerkemeier, Marc Langheinrich, Elgar Fleisch, Friedemann Mattern e Sanjay E. Sarma.

Em 2009, Salvador sediou o primeiro evento da temática no Brasil. Organizado pelo CIMATEC SENAI e pela Saint Paul Etiquetas Inteligentes, o 1º Congresso de Tecnologia, Sistemas e Serviços com RFID que aconteceu de 26 a 29 de agosto. Na segunda edição, o evento mudou de nome para Congresso Brasileiro de Internet das Coisas e RFID, que aconteceu em Búzios em outubro de 2011.

No Brasil além do congresso, 2010 marcou a implantação do COR (Centro de Operações do Rio), quartel general da prefeitura da cidade do Rio de Janeiro que opera com tecnologia de cidades inteligentes da IBM (International Business Machines).

No COR um telão de 80 m² mostra o mapa da cidade com camadas de informação e imagens de câmeras que permitem visualizar o trânsito, condições climáticas e diversas ocorrências.

Desde 2011 com a proliferação de novas tecnologias, começou a discussão sobre a criação de padrões internacionais que de fato permitam que possa existir uma rede autônoma de objetos conectados, com isso o ITU (International Telecommunication Union) das Nações Unidas, vem reunindo especialistas para a consolidação do padrão global.

Com este cenário, algumas empresas começaram a perceber que apenas automatizar sua produção não estava sendo suficiente, havia-se à necessidade que seus maquinários comunicassem entre si, que fossem inteligentes para gerar relatórios e trazer mais agilidade, tanto na comunicação entre fornecedores, como na manutenção e tempo de produção dentro da fábrica e de suas inúmeras filiais. No intuito de formar uma grande rede neural de máquinas.

Foi esta proposta que a empresa Siemens em 2016 trouxe a ideia da MindSphere[1]. Trazendo o conceito de Indústria 4.0 e estampando o seu slogan “Mind Sphere (SO de código aberto para IoT) transforma dados em conhecimento e conhecimento em negócios bem-sucedidos”.

Nos últimos anos uma grande quantidade de IoT é vendido, seja em forma de brinquedos: como drones, bonecos com chat de voz, ou até mesmo em nossos aparelhos domésticos como: liquidificador, geladeira, lâmpadas e muito mais. Trazendo uma nova realidade e cercando as pessoas de equipamentos inteligentes que trazem facilidades para o dia a dia.

Mas o foco deste trabalho não é mencionar o vasto caminho que a IOT vem percorrendo e criando raízes em vários setores, seja ele presente na Indústria, na Agricultura ou na sua casa. E sim aprofundar na IoT e sua aplicação em carros autônomos.

3 HISTÓRIA DOS VEÍCULOS AUTÔNOMOS (VA)

O caminho para a construção do carro autônomo foi desde a década de 1920, onde era necessários meios externos especiais para se fazer o carro andar sem motorista, o primeiro a aparecer foi um Houdina Radio Control, onde um carro atrás com um rádio control (controle com ondas de rádio) o controlava pelas ruas de Nova York.

Na década de 1950, os métodos preferidos pelos pesquisadores foram condução de forma elétrica, onde era colocado impulsos elétricos na pista onde o carro passava, feitos pela RCA Labs, os circuitos de detecção foram incorporados em estradas na Nova Jersey (Ricardo Caruso, 2017).

Esses circuitos foram integrados no GM Firebird II de 1956.Imagem do Firebird II ilustrado na Figura 3.

Figura 3 (Imagem meramente ilustrativa, O GM Firebird II de 1956)

Fonte: GM Heritage Center (2020)

O plano ambicioso continuou a ser desenvolvido na década de 1960, pelas Ohio State University, governo dos Estados Unidos e da Bendix Corporation (1924 - 1983, empresa que fabricou freios automotivos e aeronáuticos, sistemas elétricos e hidráulicos), onde todos estes projetos estavam focados em estradas “eletrônicas”.
Na mesma década de 60, a Universidade de Standford desenvolveu um robô para sondas lunares, com câmeras de vídeos interligado a um controle por meio de um

longo cabo, no final da década de 70 o veículo teve sua inteligência melhorada onde atravessou uma sala cheia de obstáculos como cadeiras, sem intervenção humana, por consequência, a sonda lunar parece ter sido o primeiro objeto robótico autônomo.

O Reino Unido também entrou no projeto de criar carros com estradas eletrônicas, *"drive-by-wire"*, onde os carros chegaram a marca de 130 km/h na estrada Crowthorne, em 1969. Ficou provado que o veículo tinha melhor eficiência do que conduzido por um motorista, os relatórios reivindicavam que esta tecnologia poderia prevenir em média 40% dos acidentes rodoviários.

No final da década de 1970, saiu os primeiros carros autônomos conhecidos atualmente, equipados com sensores. Processadores e comandos necessários para se locomoverem, teoricamente sem interferências externas (tráfego de carros e pessoas).

Professor Ernst Dickmanns da Universidade da Bundewehr de Munique liderou uma equipe e preparou uma van Mercedes-Benz para isso, a van foi capaz de processar a entrada das câmeras e fornece comandos para o carro, atingindo mais de 90 km/h. o veículo, chamado de VaMP (Versuchsfahrzeug für autonome Mobilität und Rechnersehen), possui 2 câmeras, oito microprocessadores intel 16-bits e um conjunto de outro sensores e softwares.

Após 7 anos, o VaMP foi apresentado com duas câmeras que processavam 320x240 pixels, onde era possível processar até 100 metros de distância, com isto o veículo reconhece as faixas das vias, sua posição e presença de outros veículos. No test-drive feito perto de Paris, o VaMP atingiu 130 km/h com um sistema de troca de faixas em um trânsito simulado.

Em 1995, a equipe de Ernst desenvolveu e adaptou um sistema de condução automática para um Mercedes S-Class. Na Figura 4 abaixo podemos ver o modelo da Mercedes daquela época.

Figura 4: Mercedes Bens S-Class

Fonte: Ernst Dickmanns

A equipe pilotou o veículo de Munique na Alemanha até Odense na Dinamarca, totalizando 1600 quilômetros e com velocidade até 180 km/h, “cerca de 95% do trajeto foi percorrido de forma automática”, diz Ernst.

3.1 Níveis de Autonomia em Veículos

De acordo com CARANDDRIVER e MotorShow, os carros autônomos têm vários níveis sendo:

- **Nível 0: sem automação**
  Direção de forma manual, motorista com total controle.
- **Nível 1: assistência ao motorista**
  Principais ações dependem do motorista, veículo possui algumas funcionalidades autónomas, mas em maior parte o motorista é quem o dirige.
- **Nível 2: automação parcial**
  Carros que estão no mercado atualmente, carro consegue ficar entre faixas, acelerar e frear, porém motorista deve estar atento pois o sistema não é totalmente seguro.
- **Nível 3: automação condicional**
  Carro possui uma alta tecnologia para dirigir em certas condições no trânsito, porém motorista deve ficar atento quando for solicitado tomar o controle.
- **Nível 4: alta automação**
  Atualmente em pesquisa, altamente autônomo, sendo possível o carro dominar tudo que necessita para dirigir, porém não tão viável com para climas ou estradas altamente perigosas.

- **Nível 5: automação completa**
  Atualmente visto em somente filmes, onde o carro dispensa o motorista e o leva para onde quiser com comandos de voz.

Embora a vinda dos carros autônomos pode ser vista como uma evolução da tecnologia atual, existem vários problemas com esta vinda, como por exemplo um hacker ou um erro de programação da empresa no sistema do carro poder levar uma ou várias vidas.

3.2 Possíveis tipos de veículos com autonomia

Atualmente está sendo estudado autonomia para veículos comuns, como carros e em pequena parte caminhões (Volvo), muitos destes veículos estão sendo transformados para elétricos, para obter as maiores vantagens possíveis na instalação de novos serviços.

É possível observar que futuramente haverá demanda para automação em veículos de grande porte e veículos de carga humana (ônibus, navios, etc) tenham sua própria automação, indo além do que há hoje, é possível dizer que a automação está longe de seu fim, a quantidade de possibilidades vai desde automatizar um carro até automatizar um foguete ou uma nave.

3.3 Importância da Segurança

Um garoto de 13 (treze) anos levou 10 (dez) minutos para conseguir tomar o controle de um drone, “Levou menos de dez minutos para eu hackear o drone e conseguir controlá-lo completamente. Essa falta de segurança é compartilhada por outros dispositivos IoT. Imagine se isso fosse feito por cibercriminosos. Se eu consegui, cibercriminosos motivados não poderiam fazer algo semelhante? ”, diz Reuben Paul. **(Rodrigues, maio 2019)**

4 FUNCIONAMENTO DO VEÍCULO AUTÔNOMO

4.1 Dispositivos

Existe uma grande quantidade de sensores utilizados para um único carro se tornar ‘parcialmente’ autônomo, vai desde: sonar, câmeras, lasers, etc.

4.1.1 Sensores Externos

Utilizados para detectar as características do ambiente, os mais utilizados são as câmeras, os radares, os sonares e os LIDARs.

- **Câmera estereoscópica**

  São câmeras que possui duas ou mais lentes que geram filme ou fotos do ambiente em diferentes perspectivas para gerar uma noção de profundidade tentando simular a visão humana.

- **Câmera Infravermelha**

  Câmeras capazes de captar o ambiente noturno de forma eficaz, ele verifica os corpos pelas suas temperaturas com sua radiação infravermelha, invisível a olho humano.

Em seguida,temos uma câmera infravermelho filmando uma rua tranquila em plena noite.

Figura 5: Visualização de uma câmera infravermelho.

Fonte: Uno Soluções em Segurança (2009)

- **Radar**

  Radar emite ondas de rádio em uma certa direção, ao retornar é possível medir a velocidade e a intensidade da onda para se ter noção do tamanho objeto a frente e sua distância.

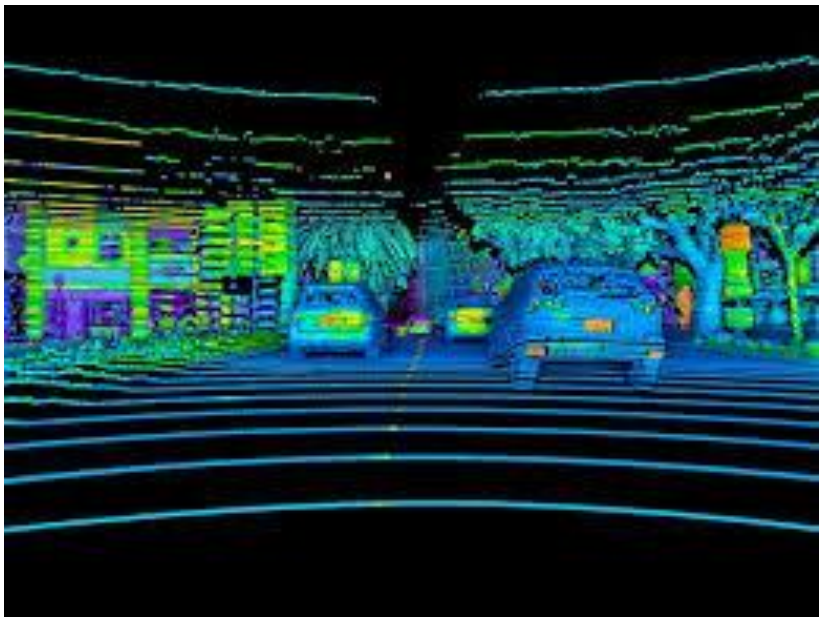
- **Sonar**

  De forma parecida do radar, sonar envia ondas sonoras pelo ambiente inaudível pelo ser humano, para medir o ambiente.

- **LiDARs**

  Possui semelhanças com Radar, somente que ao invés de utilizar ondas de rádio, ele mapeia o ambiente com feixes de luz. Ele funciona bem de dia e noite, porém possui um preço alto, o recebimento de dados do sensor LiDAR é ilustrado abaixo na figura 6.

Figura 6: Imagem retirada de um sensor LIDAR.



Fonte: The Geospatial (2019).

4.2 Visão Computacional

Quando se fala em carros autônomos, a maior dúvida que é gerada é: como o carro enxerga o mundo? Neste contexto a maior importância em como ele enxergar se dá ao “IoT” como solução ao problema.

A NVIDIA desenvolveu sistemas de suporte a esses problemas, interligar vários sensores para se obter uma imagem com as informações compiladas dos sensores, essa imagem é processada por um computador especial no carro, assim gerando os comandos necessários para a ação naquele momento.

A figura 7 mostra o carro autônomo em pleno funcionamento em uma rodovia nos Estados Unidos.

Figura 7: Imagem tirada de um carro autônomo em uma rodovia.

Fonte: NVIDIA Drive Labs (2020)

Os sensores são os sentidos que carro ganha, os animais têm sentidos através de olhos, orelhas, língua, nariz. Não é possível produzir sentidos em uma máquina, assim e usado sensores, como radares, LiDARs, sonars, etc…

Dando alguma sensação do que passa próximo aos carros, após isso é necessário processar estas informações com computadores (memória, processador e local onde salvar dados). Com informações processadas, são enviados comandos para o carro agir de acordo com a situação.

Em sua maioria. os dados são processados e melhorados por uma IA (inteligência Artificial), a IA é quem decide se os dados obtidos farão com que o veículo faça alguma ação, sem a IA o veículo pode se locomover porém será de forma insegura, e se algum acontecimento imprevisto e não programado acontecer, como o carro irá reagir? Com IA isto pode ser resolvido.

5 METODOLOGIA

O termo “hacker” quando mencionado traz pânico e negatividade para a palavra. Quando se ouve falar em hacker, logo pensamos que alguém ou um grupo

de entusiastas nerds invadiram algo sigiloso e roubou dados secretos, tratando assim dele um criminoso virtual. Mas não é bem por aí... Qualquer pessoa que se dedique intensamente em alguma área específica da computação e descobre utilidades além das previstas nas especificações originais pode ser considerado um hacker.

A origem do termo surgiu na década de 1960 nos Estados Unidos com a expressão “hack” para designar soluções inovadoras a problemas. Com o tempo foi associado a programadores de computador que estavam realizando grandes feitos no Instituto de Tecnologia Massachusetts (MIT) e em outras partes do mundo.

Os hackers ao contrário do que se pensa, utilizam suas habilidades para o bem, muitas das vezes estão ligados a setores de perícia forense, pesquisas de vulnerabilidade, engenharia de projetos, desenvolvimento de softwares, testes de invasão, gestão de risco, entre outros.

Existe algumas variações do termo, são elas:

- **White Hat (Hacker ético):** Seguem a mesma linha de pensamento do termo original, o mais importante para eles é o conhecimento, gostam de acessar informações que não está público. A maior parte do tempo passa estudando o funcionamento de protocolos, telefonia, internet ou até mesmo a criação de softwares livres como o GNU/Linux

- **Black Hat (hackers mal-intencionados) -** Esses também procuram o proibido e o inacessível, o que difere dos White Hats é o que fazem com a informação e conhecimento. Os Black Hats descobrem vulnerabilidades e utilizam delas para o bem próprio, seja para obter dados sigilosos de outras pessoas ou empresas.

- **Gray Hats (Hacker sem lado) -** Esses hackers se assemelham com ambas as categorias citadas acima, porém é uma categoria neutra. Utilizam de seus conhecimentos para explorar falhas de segurança em sistemas e chamar a atenção da empresa atacada. Não agem com intenção maliciosa, mas muitas das vezes divulgam publicamente a brecha encontrada para que criminosos exploram.

5.1 Vulnerabilidades dos carros modernos

Há muito tempo, vários estudos descreveram potenciais vulnerabilidades e a fragilidade do sistema automotivo em um contexto acadêmico Alguns estudos com pesquisadores, demonstraram usando componentes e automóveis reais, tanto no laboratório e em testes de estrada que, uma vez que um hacker acessa a rede interna,

ele ou ela pode assumir completamente o controle da ampla gama de funções automotivas, incluindo a desativação dos freios, travando seletivamente rodas individuais sob demanda parando o motor ou trancando as portas.

Em outro estudo também, foi demonstrado que ataques a sistemas de defesa alavancam fraquezas individuais, incluindo um ataque que incorpora código malicioso na unidade de telemática de um carro e que apaga completamente qualquer evidência de sua presença após um possível acidente.

Em outra pesquisa, os autores demonstraram e indicou que a rede interna do veículo pode ser acessada através de uma ampla gama de meios remotos (vetores de ataque), como Rádio celular Bluetooth, 3G usado por unidades telemáticas e canais de comunicação sem fio, além de indiretos acesso físico através do diagnóstico a bordo (OBD-II)porta.

As vulnerabilidades relatadas por pesquisas anteriores podem então serem exploradas e os automóveis podem ser controlados remotamente sem qualquer acesso físico direto. O principal motivo dessas vulnerabilidades é o controlador padrão de rede de área (CAN), desenvolvido em 1988 e atualizados em 1991 e em 2003. Há uma variedade de protocolos que podem ser implementados no barramento do veículo.

Desde 2008 todos os carros vendidos nos EUA deveriam implementar o barramento CAN (ISO 11898) para diagnóstico. CAN (grosso modo, é um protocolo de dados da camada de link) tornou-se a rede de comunicação dominante para redes de automóveis (por exemplo, usadas pela BMW, Ford, GM, Honda, Volkswagen, etc.). As ECUs (Central para controlar dispositivos mecânicos) são conectadas em rede; e em um ou mais barramentos baseados no padrão CAN.

ECUs comunicam-se entre si enviando pacotes CAN. A estrutura e o protocolo do barramento CAN foram desenvolvidos quando não havia comunicação celular ou sem fio tecnologias e automóveis não estavam conectados à rede.

Portanto, o protocolo CAN possui recursos de segurança muito fraca contra adversários externos. Hoje, porém, os sistemas automotivos têm amplo conectividade; milhões de carros nas estradas hoje podem ser endereçados diretamente por celulares e pela internet.

Para piorar, hoje em um carro moderno há uma ampla gama de funcionalidades, incluindo motor, transmissão, freios, iluminação e entretenimento controlados por uma combinação de componentes digitais ECU.

6 ESTUDOS DE CASOS

6.1 Estudo de Caso 1: Hackers desligam motor de Jipe Cherokee remotamente

Figura 8: Americanos Charlie Miller e Chris Valasek

Fonte: Wired (2020)

Um experimento em 2015, realizado por dois americanos Charlie Miller e Chris Valasek (ilustrados na figura 8), mostrou uma vulnerabilidade no sistema de conexão (Uconnect) do Jeep Cherokee. Através de acesso remoto, conseguiram ter controle a funções importantes do carro como: controle no sistema de travas da porta, controle de mídia, limpadores de pára-brisa, freio, acelerador e até mesmo ao funcionamento do motor.

A imagem abaixo (figura 9) mostra os hackers enviando uma foto para o aparelho de mídia.

Figura 9: Hackers controlam jeep remotamente

Fonte: Wired (2020)

Tudo isso é possível apenas porque a Chrysler, como praticamente todas as montadoras, está fazendo o possível para transformar o automóvel moderno em um smartphone.

O Uconnect, um recurso de computador conectado à Internet em centenas de milhares de carros, utilitários esportivos e caminhões Fiat Chrysler, controlam o entretenimento e a navegação do veículo, permite chamadas telefônicas e até oferece um ponto de acesso Wi-Fi.

Graças a um elemento vulnerável, a conexão celular do Uconnect também permite que qualquer pessoa que conheça o endereço IP do carro obtenha acesso de qualquer lugar do país. "Do ponto de vista de um invasor, é uma vulnerabilidade super agradável", diz Miller.

A partir desse ponto de entrada, o ataque de Miller e Valasek gira para um chip adjacente na unidade principal do carro - o hardware do seu sistema de entretenimento - reescrevendo silenciosamente o firmware do chip para plantar seu código. Esse firmware reescrito é capaz de enviar comandos através da rede interna de computadores do carro, conhecida como barramento CAN, para seus componentes físicos, como o motor e as rodas. Miller e Valasek afirmam que o ataque ao sistema de entretenimento parece funcionar em qualquer veículo Chrysler com o Uconnect desde o final de 2013, todo o ano de 2014 e início de 2015.

6.2 Estudo de Caso 2: “Roubo sem chave”

Figura 10: Toyota RAV4.

Fonte: Motoring Research (2019)

A empresa Europeia Thatcham Research testou em junho de 2019 sete carros e avaliou-os no quesito segurança dos veículos com sistemas de entrada sem chave.

Todos os carros foram classificados como “bons” ou melhores quando não havia sistema sem chave. No entanto, o DS3 Crossback, Mazda 3, Toyota RAV4 (figura 10) e Volvo S60 (figura 11) foram todos rebaixados para 'ruins' depois que as vulnerabilidades de entrada e inicialização sem chave foram incluídas.

Laurenz Gerger, consultor da Associação de Seguradoras Britânicas (ABI), disse esperar que os resultados mais recentes de segurança incentivem tanto os fabricantes quanto os motoristas a agir contra “a crescente questão do crime automobilístico sem chave.

Figura 11: Volvo S60

Fonte: Motoring Research (2019)

"As classificações da Thatcham mostram que, para muitos veículos, ainda há um longo caminho a percorrer para reduzir os 1,2 milhões de libras atualmente pagos todos os dias por todos os roubos de carros".

Outra pesquisa no início de 2019 realizado pelo grupo de consumidores “Wich?“ mostrou que os carros novos mais vendidos estão suscetíveis ao roubo de carro sem chaves. Os quatro grandes são Ford Fiesta, Ford Focus, Volkswagen Golf e Nissan Qashqai (Ethan Jupp, 2019).

A pesquisa abrangeu 237 modelos de carros equipados com tecnologia sem chave, entre estes, praticamente todos podiam ser abertos e iniciado com a caixas de relé, esse tipo de roubo geralmente ocorre na casa do proprietário do carro, devido à forma como ele funciona. Um dos dois ladrões fica o mais próximo possível da casa, enquanto o outro espera no carro.

A caixa transmite o sinal da chave dentro da casa para o carro. Isto engana o carro, pensando que a chave está mais próxima e a destrava, deixando-o pronto para dirigir.

6.3 Estudo de Caso 3: Auto piloto da Tesla Model 3 falha

No início de maio de 2020, um carro da empresa Tesla.Inc do visionário Elon Musk, que também realizou a missão de enviar dois astronautas a base espacial ISS utilizando foguetes reutilizáveis de baixo custo, teve problemas com Model 3 em Taiwan.

O carro acabou colidindo com um caminhão capotado na Rodovia Nacional 1. O motorista estava utilizando o piloto automático e o sistema não reconheceu o enorme retângulo parado na pista, mesmo com as condições de visibilidade não alteradas. O condutor quando percebeu, tentou acionar os freios de emergência, porém o carro não conseguiu parar a tempo.

Segundo o corpo de bombeiro do condado de Chiayi, os dois motoristas não sofreram ferimentos. No momento do acidente o veículo estava a uma velocidade de 110 KM//H.

Figura 12: Carro que colidiu com caminhão

Fonte: TecMundo (2020)

7 DISCUSSÕES

Grande parte das empresas de carros autônomos estão cientes destes problemas, como são todas empresas multinacionais que estão tendo este projeto, todas elas possuem grande segurança em seus serviços e grande quantidade de dinheiro a investir neste projeto, empresas como: Google, BMW, Volvo, Ford.

Uma grande solução que as empresas tiveram em relação ao IoT, foi a colocação de um computador completo no carro, como o carro é grande, não há necessidade de portabilidade, assim resolvendo um grande problema com limite de hardware.

Outro problema a surgir veio em relação com a quantidade de dados que os carros vão se comunicar com os servidores destas empresas, isto poderá ser resolvido com a mais nova internet 5G que está por vir.

A grande quantidade de processos que um carro irá fazer somente com a captação dos sensores será enorme, além de sua enorme quantidade de dados adquiridos em seu dia-a-dia, será necessário um chip poderoso ou somente focado nesse tipo de serviço para obter o menor tempo necessário, assim podendo fazer o carro reagir mais rápido podendo salvar vidas.

A NVIDIA veio com uma proposta como esta, com seu chip NVIDIA DRIVE AGX Orin que em teoria pode suportar 200 trilhões de operações por segundo, que poderá mudar os carros autônomos de nível 2 á nível 5, além de colocar sua IA para carros autônomos de forma Open Source.

8 EXPECTATIVAS FINAIS

Existem três possibilidades de algo acontecer no futuro sobre carros autônomos, onde: tudo deu certo, nada deu certo, acidentes aconteceram, mas projeto continua em andamento.

Tudo deu certo: neste cenário, tudo sobre planejamento dos carros autônomos, onde sua produção em empresas, seus sensores desenvolvidos de forma quase perfeita para veículos e sua inteligência artificial sendo altamente compatível e evoluída, é possível ver os carros já sendo vendidos e não havendo problemas de pós-venda sobre veículos com casos de acidentes.

Nada deu certo: neste cenário, sendo o pior possível, qualquer possibilidade de obter carros autônomos foi reduzida a quase nada, onde todos os testes e as experiências começaram bem, mas foram desencaminhando após o tempo devido a problemas com climas, sensores, inteligência artificial, etc…, neste cenário é possível observar que de alguma forma os carros autônomos foram ditos não terem futuro pelas empresas que o desenvolveram.

Acidentes aconteceram, mas projeto continua: neste caso, onde provavelmente estamos, acidentes e problemas estão acontecendo, carros podendo serem hackeados, perdendo controle, sensores dando problemas, entre outros. Projeto segue em frente, onde empresas e pessoas de todo mundo estão em uma corrida onde quem conseguir fazer seu carro de forma 100% autônoma, será o que dominará o mercado. Empresas e desenvolvedores estão fazendo cada vez mais hackathons, eventos onde pessoas de áreas específicas são convidadas a testar e procurar falhas em produtos das empresas parceiras.

CONCLUSÃO

Muito trabalho há para ser feito durante as próximas décadas. A tendência é que montadoras continuem investindo forte no desenvolvimento dessas tecnologias, em uma corrida contra o tempo, para que seja lançado o carro “ideal” do futuro. Portanto, é um dever nosso da área de Segurança da Informação acompanhar esses avanços e garantir uma boa segurança desses dados que serão gerados.

Pessoas mal-intencionadas sempre existirão, sejam elas atuando na internet diretamente ou em dispositivos tecnológicos, o que deve mudar é como lidamos com essas ações e quais serão as medidas que tomaremos para prevenção.

O ser humano aprenderá novas relações, não de humanos para humanos, mas sim de humanos para máquinas, um novo desafio que está por vir, pois a pretensão é que essas máquinas estejam presentes diariamente e frequentemente no cotidiano de cada indivíduo. Cabe aos responsáveis uma sensibilização de que máquinas não pensam, e independente da tecnologia aplicada, em momentos extremos a melhor decisão sempre será humana.

A tecnologia sempre nos ajudou em realizar nossas tarefas com maior praticidade, conectando pessoas a rede e formando um grande laço, trazendo facilidades, comodidades e levando o homem a lugares nunca antes imaginado, porém nessa pesquisa, podemos absorver uma mensagem transmitida, que é um dever de não desaprender nossas relações mais humanas. Os avanços continuaram, porém os princípios deverão ser mantidos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Israel de. **Como funcionam os carros autônomos? (Parte 1 - sensoriamento e visão computacional).** Disponível em: <https://medium.com/brasil-ai/como-funcionam-os-carros-aut%C3%B4nomos-parte-1-sensoriamento-e-vis%C3%A3o-computacional-ae25d17c66a1> Acesso em: 14 jun. 2020.

AUCOCK, Richard. **MORE new cars slammed for keyless theft flaws.** Disponível em: <https://www.motoringresearch.com/car-news/more-new-cars-slammed-keyless-theft-flaws/?fbclid=IwAR1Qzf6lqk-Wv6BbGwlZZWCuk6niX0mB2ezCPNjcK8OBq8nYhxI_u-p1PDw> Acesso em: 14 jun. 2020.

AXELSON, Dorothea. **The Social Web of Things.** Disponível em: <https://www.youtube.com/watch?v=i5AuzQXBsG4> Acesso em: 22 jun. 2020.

CARUSO, Ricardo. **Em 1925 já se falava em carro autônomo…**. Disponível em: <http://autoetecnica.band.uol.com.br/em-1925-ja-se-falava-em-carro-autonomo/>. Acesso em: 25 set. 2019.

CHARLEAUX, Lupa. **Autopilot da Tesla faz Model 3 bater em caminhão capotado [vídeo].** Disponível em: < https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/153705-autopilot-tesla-model-3-bater-caminhao-capotado-video.htm#:~:text=Autopilot%20da%20Tesla%20faz%20Model%203%20bater%20em%20caminh%C3%A3o%20capotado%20%5Bv%C3%ADdeo%5D,-02%2F06%2F2020&text=Em%20Taiwan%2C%20um%20Tesla%20Model,n%C3%A3o%20conseguiu%20evitar%20a%20batida. > Acesso em: 14 jun. 2020.

CHELLA, Marco Túlio. **Brinquedos interativos com recursos de IoT**. Disponível em: <https://saense.com.br/2017/06/brinquedos-interativos-com-recursos-de-iot/>. Acesso em: 5 nov. 2019.

CISCO. **Cisco IoT.** Disponível em: <https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html> Acesso em: 22 jun. 2020.

GM HERITAGE CENTER. **1956 Firebird II.** Disponível em: <https://www.gmheritagecenter.com/gm-vehicle-collection/1956_Firebird_II.html> Acesso em: 14 jun. 2020.

HAMMAN, Renan. **Veja quais são as 30 empresas que já estão envolvidas com carros autônomos**. Disponível em: <https://www.tecmundo.com.br/carro/103966-existem-30-empresas-envolvidas-carros-autonomos-confira-quais.htm>. Acesso em: 5 nov. 2019.

JUPP, Ethan. **Keyless theft shock: most popular cars are the easiest to steal.** Disponível em: < https://www.motoringresearch.com/car-news/keyless-theft-popular-cars-easiest-steal/ > Acesso em: 14 jun. 2020.

KASPERSKY. **Adolescente de 13 anos leva apenas 10 minutos para hackear drone**. Disponível em: <https://www.kaspersky.com.br/blog/adolescente-hacking-drone-iot/11767/>. Acesso em: 5 nov. 2019.

METAGAL. **Novos hackers: a segurança dos dados em carros autônomos**. Disponível em: <http://www.metagal.com.br/blog/dados-em-carros-autonomos/>. Acesso em: 16 out. 2019.

MOTOR SHOW. **Carros autônomos: conheça os seis níveis de automação.** Disponível em: <https://motorshow.com.br/carros-autonomos-conheca-os-seis-niveis-de-automacao/> Acesso em: 14 jun. 2020.

MUNDO MAIS TECH. **Conheça os diferentes tipos de hackers.** Disponível em: < https://mundomaistech.com.br/seguranca/conheca-os-diferentes-tipos-de-hackers/> Acesso em: 14 jun. 2020.

NVIDIA. **NVIDIA DRIVE LABS.** Disponível em: <https://www.nvidia.com/en-us/self-driving-cars/drive-labs/>. Acesso em: 14 jun. 2020.
RODRIGUES, Leonardo Cavalheiro. **FUNDAMENTOS, TECNOLOGIAS E APLICAÇÕES DE VEÍCULOS AUTÔNOMOS.** Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/8454/1/PG_COELE_2017_2_19.pdf> Acesso em: 14 jun. 2020.

PRETI, Mariana. **Como a IoT está possibilitando a Revolução dos Carros Autônomos**. Disponível em: <https://c2ti.com.br/blog/como-a-iot-esta-possibilitando-a-revolucao-dos-carros-autonomos-inovacao>. Acesso em: 25 set. 2019.

RIGUES, Rafael. **CPU Nvidia para carros autônomos é 7 vezes mais potente que a anterior.** Disponível em: <https://medium.com/brasil-ai/como-funcionam-os-carros-aut%C3%B4nomos-parte-1-sensoriamento-e-vis%C3%A3o-computacional-ae25d17c66a1> Acesso em: 14 jun. 2020.

ROBERTS, Paul. **IDC: 30 Billion Autonomous Devices By 2020.** Disponível em: <https://securityledger.com/2013/10/idc-30-billion-autonomous-devices-by-2020/> Acesso em: 22 jun. 2020.

ROSTCHECK, David. **The Self-Driving Car — from 1994.** Disponível em: <https://medium.com/@davidrostcheck/the-self-driving-car-from-1994-fb1ec617bd5a> Acesso em: 14 jun. 2020.

SIEMENS. **MindSphere - O sistema operacional aberto para IoT.** Disponível em: < https://www.youtube.com/watch?v=6sTcCev2saU > Acesso em: 14 jun. 2020.

SILVA, Leidivino Natal. **A evolução da IoT aponta para o monitoramento de dados em tempo real**. Disponível em: <https://cio.com.br/a-evolucao-da-iot-aponta-para-o-monitoramento-de-dados-em-tempo-real/>. Acesso em: 5 nov. 2019.

THE GEOSPATIAL. **Flodraulic optimizes autonomous applications with LeddarTech's LiDAR sensors.** Disponível em: <https://www.thegeospatial.in/flodraulic-optimizes-autonomous-applications-with-leddartechs-lidar-sensors>. Acesso em: 14 jun. 2020.

UNO SOLUÇÕES EM SEGURANÇA. **Câmera infravermelho Dlux DL500-80 (à noite)**. Disponível em: <https://www.youtube.com/watch?v=lNi0uDkz-Jg>. Acesso em: 10 jun. 2020.

VIAS SEGURAS. **Estatísticas nacionais de acidentes de trânsito.** Disponível em: <https://medium.com/brasil-ai/como-funcionam-os-carros-aut%C3%B4nomos-parte-1-sensoriamento-e-vis%C3%A3o-computacional-ae25d17c66a1> Acesso em: 14 jun. 2020.

WIRED. **Hackers Remotely Kill a Jeep on the Highway—With Me in It.** Disponível em: < https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.> Acesso em: 14 jun. 2020.