Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Em Sistemas Embarcados
para a Indústria Automotiva

FERNANDO FERREIRA DE FRANÇA

CONSIDERAÇÕES SOBRE A SEGURANÇA DA INFORMAÇÃO EM SISTEMAS EMBARCADOS AUTOMOTIVOS

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba
2018

FERNANDO FERREIRA DE FRANÇA

CONSIDERAÇÕES SOBRE A SEGURANÇA DA INFORMAÇÃO EM SISTEMAS EMBARCADOS AUTOMOTIVOS

Monografia de Especialização apresentada ao Curso de Especialização em Sistemas Embarcados para a Indústria Automotiva do Departamento Acadêmico de Eletrônica - DAELN, da Universidade Tecnológica Federal do Paraná - UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M.Sc. Juliano de Mello Pedroso.

Curitiba

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Sistemas Embarcados para Indústria Automotiva

TERMO DE APROVAÇÃO

CONSIDERAÇÕES SOBRE A SEGURANÇA DA INFORMAÇÃO EM SISTEMAS EMBARCADOS AUTOMOTIVOS

por

FERNANDO FERREIRA DE FRANÇA

Esta monografia foi apresentada em 06 de Dezembro de 2018 como requisito parcial para a obtenção do título de Especialista em Sistemas Embarcados para Indústria Automotiva. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. M. Sc. Juliano de Mello Pedroso
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Este trabalho também é dedicado àqueles que fizeram tudo o que havia para ser feito simplesmente porque era possível. Vocês ainda sabem quem são.

AGRADECIMENTOS

Ao Grande Arquiteto do Universo por suas grandes sacadas como a luz, a força gravitacional, o eletromagnetismo e tudo mais que permeia este vasto universo desde o *Big Bang*. Segue tudo funcionando de acordo desde então.

Aos meus pais Vilma e Sebastião, avós Eunice e Francisco (em memória), madrinhas Denise e Dayse e toda família pelo apoio incondicional e suporte em todas as minhas escolhas até aqui. A Dra. Mariana Novaes pelo seu amor, carinho, companheirismo e por ter finalmente concluído o seu doutorado.

A todos os meus professores desde sempre por seus ensinamentos que trazem o conhecimento e em especial meu orientador, Juliano de Mello Pedroso, pela disponibilidade, atenção e incentivo.

A todos os meus amigos que continuam na torcida, estando perto ou longe, em especial Jan Seidl e Rodrigo Villaverde pelas revisões, eventuais correções e orientações.

A CINQ Technologies por incentivar e apoiar o constante aprendizado.

"Aquele homem acredita saber alguma coisa, sem sabê-la, enquanto eu, como não sei nada, também estou certo de não saber."

(Platão)

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

(Bruce Schneier)

RESUMO

FRANÇA, Fernando Ferreira de. Considerações sobre a segurança da informação em sistemas embarcados automotivos. 2018. 53 p. Monografia de Especialização em Sistemas Embarcados para a Indústria Automotiva, Departamento Acadêmico de Eletrônica, Universidade Tecnológia Federal do Paraná. Curitiba, 2018.

O presente trabalho apresenta uma pesquisa bibliográfica sobre a segurança da informação aplicada aos sistemas embarcados automotivos. Com base na revisão da literatura, são apresentados os principais conceitos relacionados aos sistemas e redes de comunicação automotivas elencando suas características e utilização. Em seguida, são apresentados os principais conceitos e fundamentos relacionados com a segurança da informação, bem como o impacto da segurança nos sistemas, usuários, empresas e governos. A segurança dos sistemas embarcados automotivos é abordada através da construção e análise de um modelo de ameaças, oferecendo uma visão prática dos conceitos apresentados. Por último, são apresentadas vulnerabilidades e casos de ataques à segurança de sistemas embarcados automotivos.

Palavras-chave: Sistemas Embarcados Automotivos. Redes de Comunicação Automotivas. Segurança da Informação.

ABSTRACT

FRANÇA, Fernando Ferreira de. Considerations on cyber security in automotive embedded systems . 2018. 53 p. Monografia de Especialização em Sistemas Embarcados para a Indústria Automotiva, Departamento Acadêmico de Eletrônica, Universidade Tecnológia Federal do Paraná. Curitiba, 2018.

This project presents a research on the cyber security applied to the automotive embedded systems. Based on the literature review, the main concepts related with the automotive systems and networks are presented, focusing their main characteristics and use. Following are presented the main concepts and fundamentals related with cyber security and the impact of security on systems, users, companies and governments as well. The security of embedded automotive systems is addressed through the construction and analysis of a threat model, offering a practical overview of the concepts presented. Lastly are presented cases of vulnerabilities and security attacks to the automotive embedded systems.

Keywords: Automotive Embedded Systems. Automotive Networks. Cyber Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABS	*Anti-Lock Braking System*
ASCII	*American Standard Code for Information Interchange*
ATM	*Automatic Teller Machine*
CAN	*Controller Area Network*
CPU	*Central Processing Unit*
DARPA	*Defense Advanced Research Projects Agency*
DOS	*Denial of Service*
ECU	*Electronic Control Unit*
FPGA	*Field-Programmable Gate Array*
GDPR	*General Data Protection Regulation*
IoT	*Internet of Things*
ISO	*International Standard Organization*
IVI	*In-Vehicle Infotainment*
KES	*Keyless Entry System*
LIN	*Local Interconnect Network*
MOST	*Media Oriented System Transport*
NIST	*National Institute of Standards and Technologies*
OSI	*Open System Interconnection*
RAM	*Random Access Memory*
RFID	*Radio-Frequency Identification*
ROM	*Read Only Memory*
SAE	*Society of Automotive Engineers*
SBC	*Single Board Computer*
SEI	*Software Engineering Institute*

SoC	*System on a Chip*
TI	*Tecnologia da Informação*
TPMS	*Tire Pressure Monitor Sensor*
TTP/A	*Time-Trigger Protocol Class A*
USB	*Universal Serial Bus*
V2I	*Vehicle-to-Infrastructure*
V2V	*Vehicle-to-Vehicle*

SUMÁRIO

1 INTRODUÇÃO

Os sistemas embarcados vêm ganhando espaço na indústria automotiva ao longo dos anos, sendo responsáveis por grande parte da inovação tecnológica e representando parte significativa no custo de produção dos veículos atuais.

São sistemas com propósito específico e uso dedicado e portanto diferem dos sistemas computacionais de uso geral [1]. Possuem *hardware* baseado em microcontroladores ou dispositivos que encapsulam processador, memórias, interfaces e outros periféricos e executam *softwares* responsáveis pelas mais diversas tarefas, que vão desde o monitoramento do ambiente interno e externo do veículo, automação e controles diversos, além da segurança do veículo e seus ocupantes. Veículos de alta tecnologia possuem centenas de processadores embarcados executando milhares de linhas de código [2].

Este cenário já apresenta alto grau de complexidade, entretanto, os sistemas embarcados automotivos também são sistemas distribuídos que se comunicam entre si através de redes para a troca de informações, utilizando diversos protocolos com diferentes graus de criticidade com relação ao tempo de resposta e tolerância a falhas [3] [4]. Essas características dão suporte à crescente demanda por funcionalidades, assim como respondem à competitividade existente na indústria automotiva, que busca atender essas demandas, viabilizar novos modelos de negócios e se adequar às legislações específicas.

A segurança da informação desempenha um papel crucial no contexto dos sistemas embarcados automotivos. Esse aumento na complexidade dos sistemas traz consigo o aumento de vulnerabilidades oriundas de falhas de projeto e/ou implementação dos sistemas embarcados automotivos e não faz muito tempo que a indústria automotiva começou a levar isso em consideração [2]. O custo e complexidade relacionados, somados à falta de legislação que responsabilize as empresas por incidentes de segurança podem ser motivos para tal. Porém, novidades como o aumento na conectividade dos veículos, modelos de negócios como o consumo de informação e entretenimento por demanda, bem como a legislação que regulamenta a privacidade e proteção de dados dos consumidores, são incentivos para que a segurança da informação nos sistemas embarcados automotivos seja vista com responsabilidade e como parte essencial dos requisitos de projeto.

Motivado por esse cenário, este trabalho apresenta uma pesquisa sobre a segurança da informação no contexto dos sistemas embarcados automotivos. Com base na revisão literária específica (como SCHNEIER e STALLINGS) e aplicada (LEMKE et al), o texto percorre os principais conceitos relacionados aos sistemas e redes de comunicação automotivas elencando suas características e particularidades.

Em seguida, são apresentados os conceitos relacionados à segurança da informação.

Estes conceitos são os mesmos oriundos da Tecnologia da Informação aplicados nas mais diferentes indústrias, que tem como objetivo principal proteger os ativos das organizações através da manutenção da confiabilidade, integridade e disponibilidade dos sistemas.

Esses conceitos serão colocados em perspectiva aplicados aos sistemas embarcados automotivos, através da análise das motivações para se pensar sobre a segurança e da construção de um modelo de ameaças, que é o primeiro passo na análise da segurança de um sistema. Por último, são apresentados casos com exemplos de vulnerabilidades existentes e ataques à segurança de diversos sistemas embarcados automotivos.

1.1 OBJETIVOS

Desenvolver uma pesquisa com base na revisão literária em torno da segurança da informação aplicada aos sistemas embarcados automotivos.

1.1.1 Objetivos Específicos

a) Contextualizar os sistemas embarcados e redes de comunicação automotivas ao longo de sua evolução tecnologica, complexidade e aplicações;

b) Apresentar a segurança da informação como um processo que começa na fase de projeto de um sistema e se estende ao longo de todo seu ciclo de vida;

c) Demonstrar como a segurança da informação pode ser aplicada no contexto dos sistemas embarcados automotivos.

2 FUNDAMENTOS E PRINCIPAIS CONCEITOS

A seguir serão apresentados os conceitos e definições que, com base na revisão da literatura, servirão como fundamentos ao longo de todo o trabalho.

2.1 SISTEMAS EMBARCADOS

Podemos definir um sistema como um agrupamento de elementos independentes e organizados com um propósito. Na engenharia esses sistemas são unidades funcionais com entradas e saídas específicas, delimitados no tempo e espaço, atuando em um ambiente também específico na execução de tarefas previamente estabelecidas.

Sistemas embarcados são sistemas computacionais compostos por *hardware* e *software* dedicados, programados para a realização de tarefas específicas geralmente ligadas ao controle e operação de outros sistemas maiores, dos quais são parte [1].

Diferem de outros sistemas de uso geral como computadores pessoais por sua interface com o usuário limitada, também por seus componentes internos que não estão diretamente acessíveis ao usuário e pela aplicação e comportamento restritos ao propósito original para os quais foram concebidos [1].

Podem ser baseados em microcontroladores ou em SoCs (*System on a Chip*), que encapsulam processador dedicado, memória de acesso aleatório (*Random Access Memory, RAM*), memória somente para leitura (*Read Only Memory, ROM*), portas de entrada e saída (E/S) e barramentos de comunicação integrados em um único dispositivo. Entretanto, também existem sistemas embarcados do tipo *single board computer* (SBC) que possuem esses componentes dispostos individualmente, como em computadores de uso geral [1].

São exemplos de tarefas executadas por sistemas embarcados: operações matemáticas para o processamento de dados, manipulação e gestão de tempo como entrada do sistema (medindo período) ou saída (gerando formas de onda), operações de entrada e saída em tempo real para medição e controle, processamento digital de sinais e comunicação de dados [1].

Com o avanço da eletrônica, a complexidade dos sistemas embarcados aumentou assim como sua adoção, sendo muitas vezes utilizados em aplicações com requisitos de computação em tempo real, que necessitam da garantia de um tempo de resposta conhecido para a realização de uma determinada tarefa. Essa garantia de tempo só poderá ser dada se o comportamento do sistema puder ser previsto (sistema determinístico).

Dentro desse contexto é possível destacar como as principais propriedades dos sistemas embarcados [1]:

a) Geralmente baseados em microcontroladores;

b) Propósito dedicado;

c) Executado em tempo real;

d) Operações de entrada e saída são importantes;

e) Produzidos em alto volume e baixo custo;

f) Estáveis e confiáveis;

g) Baixo consumo de energia;

h) Dimensões e peso reduzidos.

Por essas características e pela capacidade de interagir com o mundo real através de sensores e atuadores, são empregados em várias áreas como: automotiva, aeroespacial, agrícola, controle industrial, médica, nuclear e hoje também estão presentes em produtos para consumo e uso pessoal diário, que trouxe o advento da Internet das Coisas (*Internet of Things, IoT*).

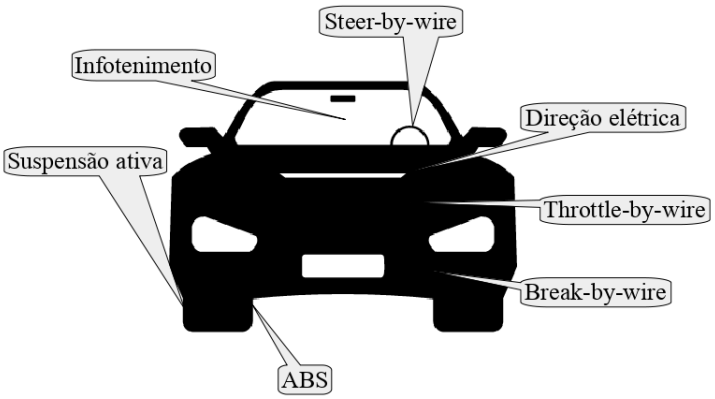
2.2 SISTEMAS EMBARCADOS AUTOMOTIVOS

A tecnologia da informação, definida aqui de forma ampla como sendo sistemas computacionais baseados em *hardware* e *software*, ganhou espaço ao longo dos anos através dos sistemas embarcados e se tornou a nova força motriz da indústria automotiva. Cerca de 90% de sua inovação é baseada em *hardware* e *software*, sendo que veículos de alta tecnologia possuem em média 80 processadores embarcados e essa tecnologia já responde por quase 50% de seu custo de produção [2].

Os sistemas embarcados automotivos estão presentes nos veículos desempenhando funções primárias como: controle do motor, transmissão, direção, estabilidade, freios e emissões de poluentes. Também atuam em funções secundárias e de conforto como janelas, retrovisores, assistência para estacionamento e climatização, além de integrar funções de entretenimento multimídia, navegação e informações gerais ao usuário (*In-Vehicle Infotainment*, IVI). Já em veículos comerciais como caminhões, além de todas as funções já descritas, atuam também no controle e monitoramento de frota através do uso de tacógrafos digitais, equipamentos regulamentados por legislações específicas que monitoram e controlam a velocidade e o regime de trabalho do veículo e seu condutor [2] [3].

O emprego dos tacógrafos digitais em substituição aos modelos analógicos anteriores, e a substituição dos tradicionais comandos exclusivamente hidráulicos e mecânicos por comandos eletrônicos e eletromecânicos das funções *x-by-wire* (*steer-by-wire*, *break-by-wire*, *throttle-by-wire*, *shift-by-wire*), representam grandes avanços da indústria no que diz

Figura 1 – Sistemas embarcados automotivos



Fonte: Adaptado de [4].

respeito a segurança tanto do veículo quanto de seus ocupantes e por esse motivo tem alto grau de criticidade [3].

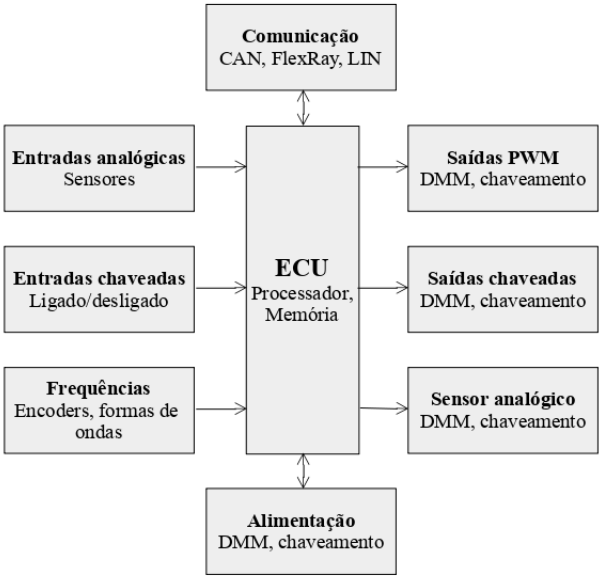
Sistemas críticos possuem requisitos de operação restritos em aspectos como tempo de resposta e tolerância a falhas. Tolerância a falhas diz respeito a capacidade de um sistema continuar operando ainda que algum dos seus componentes venha a falhar, esse requisito poderá ser alcançado através do uso de sistemas redundantes que podem assumir a função do sistema primário defeituoso, por exemplo, sistemas *steer-by-wire* e *break-by-wire* contam com sistemas mecânicos redundantes [3].

Quanto ao tempo de resposta restrito podem ser utilizados sistemas em tempo real (*hard real-time*), que apresentam uma latência pequena e previamente conhecida na execução de uma tarefa, diferentemente de sistemas *soft real-time*, onde as tarefas são executadas com base em prioridades [1].

As unidades de controle eletrônico (*Electronic Control Unit*, ECU) são sistemas embarcados responsáveis pela operação dos vários subsistemas automotivos, realizando aquisição de dados através de sensores, processamento e transmissão de mensagens pelas diversas redes de comunicação e controle através de atuadores. A figura 2 apresenta o diagrama de blocos de uma ECU com algumas das possíveis interfaces e periféricos de entrada e saída.

As ECUs são divididas por domínios de aplicação, por exemplo: controle do motor, *air-bags*, emissões de poluentes, podendo ainda ser combinadas dependendo da complexidade e da necessidade da aplicação, por exemplo: os algorítmos utilizados no monitoramento e controle da manutenção da estabilidade do veículo e prevenção do travamento das rodas (*Anti-Lock Braking System*, ABS) podem ser executados em conjunto na ECU do sistema de freios [6].

Figura 2 – Diagrama de blocos de uma ECU



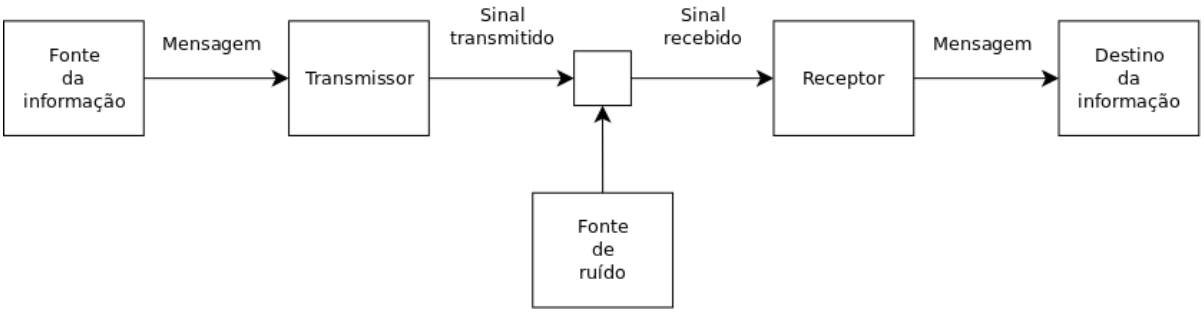
Fonte: Adaptado de [5].

Além da substituição dos tradicionais sistemas elétricos, mecânicos e hidráulicos, os sistemas embarcados automotivos vêm sendo também empregados no entretenimento e na automação dos veículos, oferecendo cada vez mais conforto, serviços e segurança aos usuários e se tornando por consequência sistemas cada vez mais complexos, esse cenário e tendências serão analisados ao longo dos próximos capítulos.

2.3 COMUNICAÇÃO ENTRE SISTEMAS E REDES DE COMUNICAÇÃO

Para que ocorra a troca de informações entre sistemas distintos é necessário que exista um meio de comunicação entre eles. A figura 3 apresenta o diagrama de blocos de um sistema genérico de comunicação.

Figura 3 – Diagrama de blocos de um sistema de comunicação



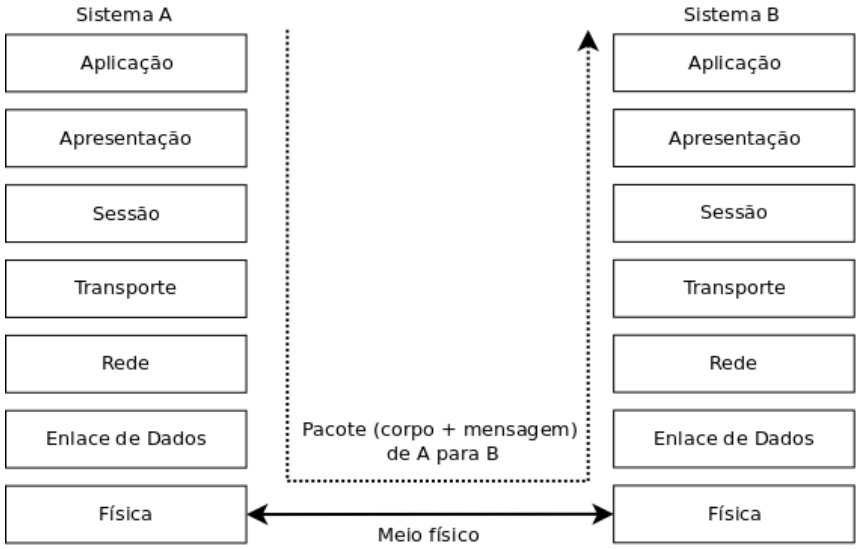
Fonte: Adaptado de [7].

No diagrama, a fonte da informação produz uma mensagem ou sequência de mensagens a serem enviadas para o receptor. O transmissor manipula a mensagem de forma a produzir um sinal compatível com o canal de transmissão utilizado, na maioria das vezes serão sinais elétricos ou ondas eletromagnéticas que podem ser propagadas através de diversos meios físicos como por exemplo cabos feito de material condutor, do ar ou fibra óptica.

O sinal transmitido estará sempre sujeito a interferências causadas por diversas fontes de ruídos, que também precisam ser consideradas e tratados de acordo. Ao receber o sinal transmitido, o receptor executa o caminho inverso do transmissor, decodificando e reconstruindo a mensagem original que será entregue posteriormente ao destino [7].

Para que esse modelo genérico funcione, os dois sistemas em questão precisam necessariamente adotar um padrão comum na comunicação. Dessa forma, foi proposto pela ISO (*International Standard Organization*) um modelo de referência em camadas que especifica padrões que vão desde o nível físico, mais baixo, até o nível de aplicação, o mais alto. O modelo OSI (*Open System Interconnection*) oferece a referência necessária para que os mais diversos equipamentos (*hardware*) e sistemas computacionais (*software*) troquem mensagens entre si. O modelo supõe que cada camada seja responsável por seus processos, se comunicando com as camadas adjacentes, recebendo e transmitindo o resultado do seu trabalho, conforme ilustrado na figura 4 [4] [8] [9].

Figura 4 – Modelo de referência OSI



Fonte: Autoria própria.

a) Física: é a camada mais baixa, lida com as características físicas (mecânica e elétrica) e manipula os sinais que serão codificados e decodificados durante a comunicação da cadeia de bits.

b) Enlace de dados: interliga e gerencia as conexões entre a camada física e a camada de rede promovendo controle de fluxo de dados, erros e endereçamento das interfaces físicas para a camada superior.

c) Rede: fornece os serviços de endereçamento e roteamento.

d) Transporte: manipula os dados que serão enviados ou recebidos em forma de pacotes. Oferece serviços orientados à conexão, onde transmissor e receptor enviam pacotes de controle que estabelecem uma conexão antes da troca de pacotes de dados propriamente dita e serviços não orientados à conexão, onde não há essa troca prévia de pacotes de controle e pontanto os dados podem ser entregues mais rapidamente, entretanto, sem garantias de entrega ou controles de fluxo e erro.

e) Sessão: estabelece, sincroniza e gerencia a sessão para troca de dados entre as aplicações, caso uma transmissão seja interrompida, poderá ser retomada a partir do último ponto de sincronização.

f) Apresentação: é responsável pela apresentação dos dados para as aplicações, aplicando codificação (por exemplo ASCII) e compressão de dados.

g) Aplicação: é a camada mais alta, fornece serviços de abstração dos processos da comunicação de dados para as aplicações.

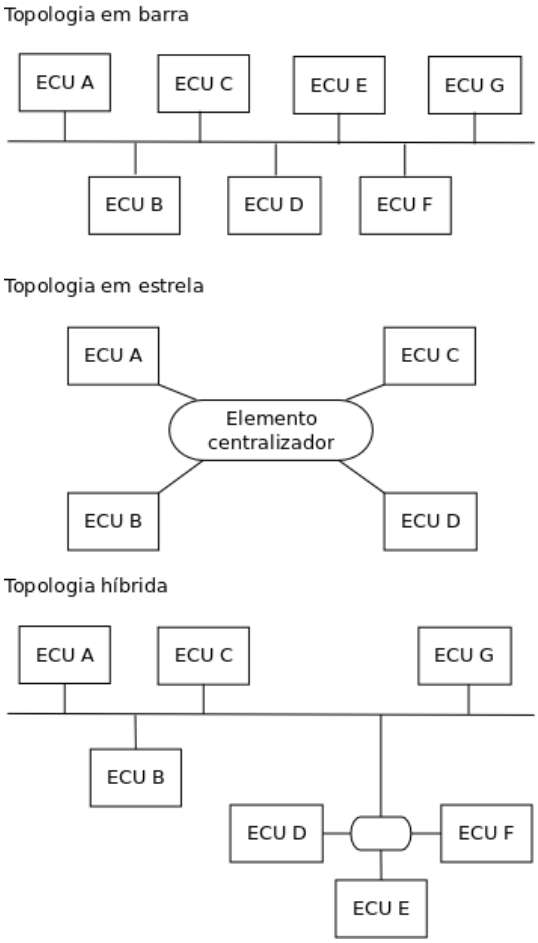
As mensagens trocadas entre as camadas são baseadas em protocolos que definem o formato, a ordem e as ações necessárias para que aconteça a comunicação [9]. Diversos protocolos são implementados tomando como referência esse modelo, permitindo que sistemas distintos se comuniquem através da troca de pacotes que trazem encapsulados na forma do protocolo em questão um cabeçalho com informações de controle e um corpo contendo a mensagem a ser transmitida.

A medida que os sistemas se interconectam através dos diversos meios físicos e utilizam protocolos para troca de mensagens temos então uma rede de comunicação. Estas podem apresentar vários arranjos físicos e lógicos (ou topologias), a depender da disposição dos seus elementos e do propósito para o qual foram concebidas. Pode-se citar como topologias de redes frequentemente utilizadas: barra, estrela e híbrida, conforme a figura 5.

2.4 REDES DE COMUNICAÇÃO AUTOMOTIVAS

As redes de comunicação automotivas são formadas pelas diversas ECUs presentes nos veículos conforme apresentado na seção anterior, e até o início da década de 1990 as informações eram transmitidas entre as ECUs em conexões ponto a ponto. Essa estratégia de interconexão se mostrou insuficiente pois ao passo que o número de ECUs aumentava, também aumentavam os problemas causados pela complexidade física das conexões como o

Figura 5 – Topologias de redes de computadores



Fonte: Adaptado de [4].

peso e a confiabilidade dos cabos e conectores [10], aspectos que podem ser determinantes em veículos.

Logo as redes de comunicação automotivas se mostraram como uma solução adequada para estes problemas, pois permitiriam o uso de um meio físico comum para a comunicação entre as ECUs. Os sistemas automotivos são divididos em domínios específicos onde cada um possui seus próprios requisitos para comunicação, entretanto é comum que dados como sinais medidos por sensores de algumas ECUs sejam compartilhados com outros subsistemas a fim de implementar ou melhorar alguma funcionalidade.

Sistemas como *powertrain* (controle de motor e transmissão) e *chassis* (suspensão, direção e freios) estão relacionados com a segurança do veículo e seus ocupantes e pontanto demandam comunicação em tempo real, além de tolerância a falhas. O sistema de *powertrain* em veículos pesados traz consigo alta complexidade também por conta de legislações específicas de controle de emissão de partículas e eficiência energética (EURO 5), exigindo que se implemente períodos de amostragem na ordem de milissegundos [10].

Já os sistemas presentes na carroceria, aqueles ligados ao conforto interno (central de comando, ar condicionado, luzes, portas, assentos), possuem requisitos de comunicação menos exigentes, geralmente trocando pequenos pacotes de dados.

Para atender os diversos cenários e seus requisitos, em 1994, a SAE (*Society of Automotive Engineers*) criou classificações para as redes de comunicação usadas na indústria automotiva com base nas várias aplicações existentes. Taxa de transmissão, tolerância a falhas, requisitos de tempo, controles de fluxo de dados, erros na comunicação e de acesso ao meio físico são algumas das características que classificam os protocolos de comunicação disponíveis [4] [10] [11].

Redes classe A possuem taxas de transmissão abaixo de 10k bit/s, sendo geralmente empregadas na comunicação de sinais simples com tecnologias de baixo custo em aplicações não críticas como controle de vidros e retrovisores. São exemplos os protocolos LIN (*Local Interconnect Network*) e TTP/A (*Time-Trigger Protocol Class A*).

As redes classe B são aplicadas em sistemas de diagnóstico e comunicação entre ECUs, com taxas de transmissão entre 10k bit/s e 125k bit/s. Protocolos como SAE J1850 e *low speed* CAN (*Controller Area Network*) já apresentam alguma tolerância a falhas através da proteção contra ruídos. O protocolo CAN é um dos mais utilizados nas redes de comunicação automotivas e foi desenvolvido pela empresa Bosch na década de 1980 para interconexão de ECUs, permitindo uma drástica redução da quantidade e do comprimento de fios e cabos utilizados até então nos veículos [10].

Os sistemas de alta criticidade utilizam as redes classe C, que além de tolerância a falhas atendem requisitos de tempo real críticos (*hard real-time*) e altas taxas de transmissão. São aplicados em sistemas como controle de *chassis*, *powertrain* e *x-by-wire* com velocidades de 1M bit/s (*high speed* CAN), 10M bit/s (*FlexRay*), emprego de cabos blindados, fibra óptica e redundância de canal de comunicação.

A comunicação sem-fio também está presente no domínio das aplicações automotivas no uso da tecnologia RFID (*Radio-Frequency Identification*) em sistemas imobilizadores anti-furto e de monitoramento da pressão dos pneus, TPMS (*Tire Pressure Monitor Sensor*), além de sistemas de entretenimento e informação multimídia que utilizam comunicação Bluetooth e permitem que o veículo se conecte com telefones celulares [4] [12].

A comunicação entre veículos (*Vehicle-to-Vehicle*, V2V) e entre dispositivos de infraestrutura de vias (*Vehicle-to-Infrastructure*, V2I) também faz uso de redes sem-fio e permite que informações relacionadas a segurança e condições das vias de tráfego sejam compartilhadas. Esse tipo de aplicação bem como o uso de telemetria já são uma realidade nos Estados Unidos, Europa e Japão [11].

Aplicações multimídia necessitam de maior capacidade de transmissão pois trafegam dados volumosos. Protocolos como o MOST (*Media Oriented System Transport*) suprem

esse requisito e entregam velocidades de transmissão na ordem de 24M bit/s através de fibra óptica [12].

A tabela 1 apresenta um comparativo entre protocolos de várias classes, com base na complexidade das aplicações automotivas e levando em consideração as diferentes faixas de custo.

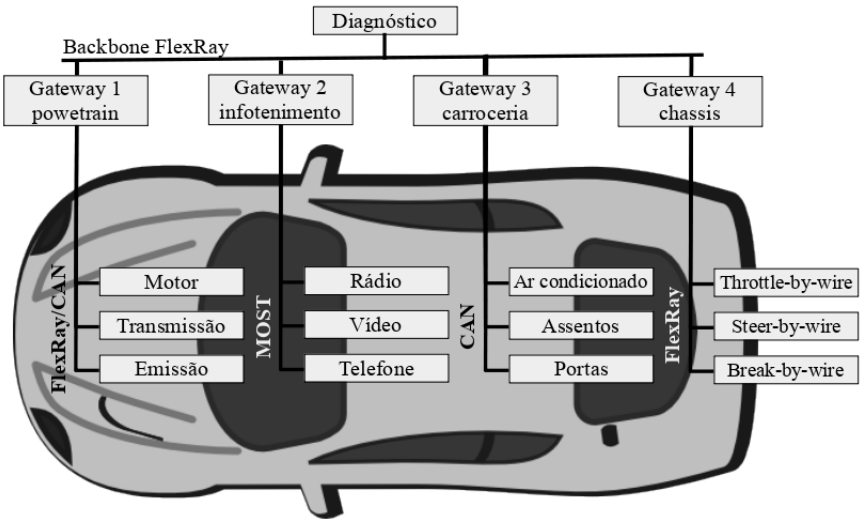
Tabela 1 – Comparação entre protocolos de comunicação automotivos

Protocolo	**LIN**	**CAN**	***FlexRay***	**MOST**
Número de fios	1	2	2 ou 4 (fibra óptica)	2 (fibra óptica)
Velocidade	40k bit/s	1M bit/s	10M bit/s	24M bit/s
Custo por nó	baixo ($1.5)	médio ($3)	alto ($6)	médio/alto ($4)
Aplicação	vidros elétricos	diagnóstico	*x-by-wire*	multimídia

Fonte: Adaptado de [13] e [14].

É possível enxergar um veículo como um sistema distribuído, composto por diversos subsistemas que são responsáveis por seus domínios específicos e se conectam através de elementos centralizadores (*gateways*) para comunicação entre si e com o ambiente externo, conforme apresentado na figura 6.

Figura 6 – Redes de comunicação automotivas



Fonte: Adaptado de [4].

2.5 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é uma área ampla de estudos aplicada a tecnologia da informação. Tem como objetivo a proteção de ativos das organizações (equipamentos, informações e pessoas) e através da gestão, monitoramento e controle busca minimizar perdas de qualquer natureza que possam se traduzir em prejuízos [15].

Hoje associamos segurança e tecnologia da informação ao ler uma notícia sobre vazamento de dados de usuários em um *website* ou uma falha grave de *software* que foi explorada em um famoso e não tão seguro sistema operacional presente em muitos computadores, a segurança da informação permeia nosso dia a dia e está cada vez mais presente nestes e em outros cenários que podem não ser de simples associação.

De acordo com o manual de segurança da NIST (*National Institute of Standards and Technologies*), segurança de computadores é a proteção aplicada a um sistema de informação com objetivo de preservar a integridade, a disponibilidade e a confidencialidade dos seus recursos: *hardware*, *software*, *firmware*, telecomunicações e informações [16].

O que há em comum entre um banco, uma base militar, um hospital, uma planta industrial, nossas residências e um veículo automotivo é o fato de que todos esses dependem cada vez mais da tecnologia da informação [17]:

a) Toda operação dos bancos depende de sistemas computacionais com alto grau de criticidade com relação a segurança seja nos seus sistemas internos, nos terminais de autoatendimento (*Automatic Teller Machine*, ATM), no acesso via Internet e meios de pagamento disponibilizados para o comércio e seus clientes.

b) Instalações militares contam com alta tecnologia e segurança tanto em computação quanto em telecomunicações. A logística e a gestão de informação também dependem de segurança por exemplo no controle de acessos.

c) No dia a dia do hospital é necessário lidar com informações sensíveis dos pacientes, logo a privacidade é uma das principais preocupações assim como a integridade dessas informações e a disponibilidade dos sistemas computacionais.

d) Uma planta industrial necessita garantir a segurança de sua operação bem como dos seus funcionários. A automação industrial é uma importante ferramenta que permite o monitoramento e o controle dos diversos sistemas presentes no chão de fábrica.

e) Muitos eletro-eletrônicos em nossas casas estão conectados a Internet. Hoje é possível monitorar as residências a distância e sistemas de automação residencial juntamente com a Internet das Coisas criaram novas possibilidades e facilidades para o dia a dia.

f) Como vimos até agora, os veículos estão cada vez mais dependentes dos sistemas embarcados. Estes controlam desde funções básicas ligadas ao conforto e entretenimento dos passageiros como também sistemas críticos ligados a segurança, eficiência e emissões de poluentes. A automação dos veículos já é uma realidade e juntamente com a telemetria entrega cada vez mais inteligência aos usuários [18].

Todas as aplicações e situações citadas estão presentes no nosso cotidiano e basicamente interagem ou são controladas por sistemas. A definição de sistema apresentada anteriormente continua válida, mas ao mesmo tempo pode não ser clara pela sua vasta abrangência, logo, os seguintes exemplos práticos são úteis para materializar esse conceito [17]:

a) Um produto ou componente (*hardware*) como uma ECU automotiva ou um *smartcard* bancário.

b) Uma rede de comunicação ou um *software* como um protoloco de comunicação, protocolo de criptografia ou sistema operacional.

c) Um *software* como um aplicativo para celular, um navegador *web* ou sistema de controle financeiro empresarial.

d) Todos os citados anteriormente incluindo as pessoas que ao interagir com estes podem desempenhar papel operacional, administrativo ou técnico seja em um ambiente interno ou externo no qual onde se encontra o sistema.

e) Todos os citados anteriormente incluindo as empresas e seus diversos departamentos e áreas específicas.

A segurança da informação possui como seus pilares a confidencialidade, integridade e a disponibilidade que, juntamente com a autenticidade, autenticação, controle de acesso e irrevogabilidade ou não-repúdio, são os conceitos mais importantes [15] [17] [19].

a) Confidencialidade: assegura que uma informação transmitida por um canal de comunicação será conhecida somente pelas partes envolvidas. Pode ser alcançada através do emprego da criptografia seja para a troca de mensagens ou armazenamento de informações. Está relacionada com o sigilo e a privacidade, permitindo que as partes envolvidas controlem a divulgação dessas informações.

b) Integridade: assegura que os dados contidos em uma mensagem não foram alterados por terceiros ou por erros, e no caso de sistemas, assegura que este execute suas tarefas livre de manipulações. Pode ser alcançada através do emprego de funções *hash* criptográficas.

c) Disponibilidade: assegura que os serviços oferecidos por um sistema estejam disponíveis para um usuário autorizado no momento do seu acesso. O nível de disponibilidade de cada sistema pode variar e o emprego de estratégias de redundância contra falhas e balanceamento de carga de trabalho podem ser utilizadas para aumentar a disponibilidade de um sistema.

d) Autenticidade: assegura que a informação é genuína e capaz de ser verificada, assim como sua fonte.

e) Autenticação: é um serviço que garante a autenticidade em uma comunicação entre as partes envolvidas, impedindo por exemplo que um terceiro não autorizado participe da comunicação interferindo na transmissão ou recepção da mensagem.

f) Controle de acesso: é um serviço que restringe o acesso a recursos do sistema para que somente as partes devidamente identificadas e autorizadas possam utilizá-los.

g) Irrevogabilidade: é um serviço que impede que qualquer uma das partes envolvidas em uma comunicação negue sua participação, provando que a mensagem foi enviada e recebida pelas partes correspondentes.

É possível classificar os diferentes níveis de impacto sobre as organizações e os indivíduos quando há quebra da segurança nos sistemas, levando em consideração os conceitos apresentados [19]:

a) Baixo: representam efeitos adversos e temporários com degradação na capacidade de operação das organizações, danos e perdas financeiras limitadas e menores prejuízos aos indivíduos.

b) Moderado: representam efeitos adversos graves e significativos na capacidade de operação das organizações, danos e perdas financeiras expressivas e prejuízos relevantes aos indivíduos que não se traduzem em lesões graves ou risco de morte.

c) Alto: representam efeitos adversos muito graves ou catastróficos na capacidade de operação das organizações, grandes danos e perdas financeiras assin como grandes prejuízos aos indivíduos que podem incluir lesões graves com risco de morte.

A segurança de sistemas aborda as ferramentas, processos e métodos necessários para desenhar, implementar e testar os sistemas, tornando-os adaptáveis a medida que o ambiente onde se encontram evolui. Diz respeito a construir sistemas que se mantenham confiáveis em situações adversas causadas por agentes internos ou externos de forma acidental ou intencional.

Os protocolos de segurança especificam os passos que devem ser seguidos pelos diversos agentes com objetivo de garantir a confiabilidade dos sistemas, um exemplo simples de protocolo é a autenticação de um usuário através de senha. Pode ser caro e complexo proteger um sistema contra todos os possíveis ataques, então geralmente os protocolos são elaborados levando em consideração algumas premissas sobre determinadas ameaças, basicamente respondendo as questões: o modelo de ameaças é realista? Como o protocolo lida com a ameaça [17]? Para elaborar um protocolo de segurança, é necessário conhecer os seguintes conceitos relativos ao sistema em questão [15]:

a) Vulnerabilidade: uma fragilidade presente no sistema que ao ser explorada poderá comprometer sua confidencialidade, integridade ou disponibilidade.

b) Ameaça: é o potencial de uma origem específica em ter sucesso ao explorar uma vulnerabilidade do sistema.

c) Agressor: intenção e método direcionados a explorar uma vulnerabilidade do sistema. Podem ser agentes humanos (por vandalismo, sabotagem ou erro na operação do sistema), ou fatores técnicos (falhas de *hardware* ou *software*) e físicos (catástrofes naturais, falhas estruturais ou em serviços públicos como telecomunicações e fornecimento de energia elétrica).

d) Risco: consciência de eventos futuros que podem causar danos ao sistema. Podem ser reduzidos através da gestão de riscos com a adoção de contramedidas.

e) Exposição: é a exploração de uma vulnerabilidade por um agressor.

f) Contramedidas: atitudes adotadas para minimizar os riscos ou minimizar o impacto de uma exposição como parte de um plano de gestão de riscos.

Um modelo de ameaças é o processo de identificação e documentação das possíveis ameaças presentes no sistema [20], levando em consideração sua superfície de ataque, que são aspectos em potencial para exploração de vulnerabilidades. Uma vez que as ameaças foram identificadas, compreendidas e categorizadas, será possível definir estratégias que permita mitigá-las.

A medida que a tecnologia avança os sistemas vão ficando mais complexos, e a complexidade dos sistemas não é algo que colabore para sua segurança. A tecnologia não é mais somente uma ferramenta, mas sim parte do risco que as organizações precisam gerenciar. Como foi apresentado, uma vez que os sistemas começam a interagir e se comunicar com outros sistemas, isso também adiciona outra camada de complexidade.

3 SEGURANÇA APLICADA AOS SISTEMAS EMBARCADOS AUTOMOTIVOS

O capítulo anterior apresentou os sistemas embarcados automotivos, situando-os dentro de um contexto mais amplo, além de delimitar o escopo de nossa abordagem dentro da segurança da informação. Tanto os sistemas embarcados automotivos quanto as redes de comunicação que os interligam se apresentam como uma solução natural para a realidade da indústria automotiva que busca evoluir tecnologicamente, solucionar problemas e entregar valor para o mercado consumidor.

Ao mesmo tempo que a tecnologia da informação e as telecomunicações fornecem as soluções para a indústria automotiva, trazem consigo também as mesmas dificuldades já enfrentadas por outros segmentos, e estas algumas vezes são específicas de cada setor. Novas tecnologias viabilizam novas oportunidades e modelos de negócios, mas também apresentam novos riscos e ameaças que precisam ser levadas em consideração, e certamente as demandas e dificuldades enfrentadas por instituições bancárias não serão as mesmas da indústria automotiva.

A medida que os sistemas embarcados automotivos evoluem, estes se tornam maiores e mais complexos comunicando e interagindo com outros sistemas, podendo apresentar comportamentos que não foram previstos por seus projetistas. Estes comportamentos eventualmente vão se traduzir em falhas ou mal funcionamento, popularmente conhecidos como *bugs*. Todas esses elementos exercem grande influência na segurança dos sistemas em geral uma vez que a complexidade é a pior inimiga da segurança, ao passo que os sistemas ficam mais complexos, eles necessariamente se tornam menos seguros [21].

Esse capítulo tem por objetivo abordar a complexidade dos sistemas embarcados automotivos sob a perspectiva da segurança da informação e o seu impacto não somente na indústria automotiva mas em outras áreas da nossa sociedade.

3.1 MOTIVAÇÕES, OPORTUNIDADES E MODELOS DE NEGÓCIOS

O que motiva uma empresa ou todo um segmento de empresas a ter uma preocupação real e efetiva com a segurança dos sistemas que desenvolvem ou utilizam? A segurança da informação, apesar de ser uma realidade nas empresas que desenvolvem, integram ou utilizam sistemas de TI, ainda é uma preocupação recente se comparada com a indústria automotiva [2].

A medida que as empresas e organizações crescem e, como parte da globalização, começam a competir em mercados internacionais, precisam observar e se adequar a normas, padrões e legislações que vão além do seu próprio conjunto de normas e práticas internas. Precisam também zelar pela sua imagem em relação a sociedade em geral e a

seus investidores e mercado consumidor em partircular.

Esses motivos iniciais seriam por si só suficientes para que uma empresa se preocupe com a segurança da informação, uma vez que violações de segurança podem facilmente se traduzir na degradação dos produtos fornecidos ou serviços prestados, gerando publicidade negativa com danos a reputação junto a sociedade, insatisfação e danos a confiança dos clientes e investidores, consequências legais e perda de receita [15] [21].

A tecnologia desempenha um papel importante nas empresas mas muitas vezes não é vista como tal. Logo a segurança da informação, que é uma área multidisciplinar e em constante evolução, recebendo as novas tecnologias e suas vulnerabilidades, demanda por parte das empresas atenção cada vez mais dedicada e o emprego de profissionais com treinamento específico, constante atenção e atualização. Evidentemente que isso tem um custo e esse investimento não é necessariamente perceptível pelo mercado consumidor.

A indústria automotiva, por força da legislação nos países, tem como principais preocupações a segurança dos ocupantes dos veículos assim como a adequação as normas de emissões de poluentes, e geralmente casos onde há alguma não conformidade com essas leis geram muita repercussão negativa, vide o caso da Volkswagem em 2015 no escândalo conhecido como *dieselgate*, onde a empresa foi acusada de tentar burlar a legislação de emissão de poluentes através de uma manipulação implementada por *software* [22].

A segurança da informação não vinha como uma preocupação prioritária na indústria automotiva até o momento por alguns motivos: muitos sistemas automotivos não demandavam preocupação com sua segurança uma vez que desempenhavam papéis muito simples e, uma tendência comum de ver a segurança da informação como desnecessária, uma vez que o objetivo principal do sistema seja alcançado [2]. Este último é um problema compartilhado também com os sistemas computacionais em geral.

Outra prática comum presente também na indústria automotiva é a de optar pela segurança baseada na obscuridade, ou seja, desenvolver soluções proprietárias para resolver problemas de segurança e não permitir que essas soluções sejam eventualmente testadas pela comunidade especializada, ao invés de buscar no mercado soluções já existentes e comprovadamente eficientes. Um sistema realmente seguro se mantém preservado mesmo que sua arquitetura seja pública [21].

Não são raros os casos onde soluções de segurança foram postas a prova pela comunidade e foram encontradas falhas graves, e não são raros também os casos onde as empresas se preocuparam somente em ocultar as falhas e processar os responsáveis pela exposição destas [11].

Em 2013 o algoritmo utilizado no sistema de criptografia *Megamos*, desenvolvido pelas empresas Volkswagen e Thales, foi quebrado pelo pesquisador em segurança Flavio D. Garcia, da Universidade de Birmingham. O sistema desenvolvido em 1997 utiliza algoritmo

proprietário com chave criptográfica de 96 bits e está presente em veículos das marcas Porsche, Audi, Bentley e Lamborghini. Na ocasião, os autores escreveram um artigo sobre o ataque que resultou na quebra do sistema e notificaram as empresas responsáveis 9 meses antes de sua publicação. As empresas então processaram os autores que foram condenados mesmo tendo se oferecido a colaborar na correção das vulnerabilidades exploradas. O algorítimo em questão ainda está no mercado presente em muitos carros [11] [23]. Veremos ainda em detalhes ao longo desse trabalho outros exemplos de ataques a segurança de sistemas automotivos.

Entretanto novas demandas para a indústria automotiva continuam surgindo, seja por parte dos governos através de leis como a regulamentação geral sobre a proteção de dados na Europa (GDPR), do mercado consumidor e pela própria indústria com o objetivo de viabilizar novas oportunidades e modelos de negócios. Logo, a segurança da informação não pode e não deve ser vista como um produto mas sim como um processo que requer responsabilidade e comprometimento ao longo do desenvolvimento dessas soluções [21].

As melhorias vêm em muitos casos como resultado dessas demandas e não por pura iniciativa baseada somente na adoção de novas tecnologias, logo, a segurança não é necessariamente um problema que a tecnologia possa resolver. Se por um lado pode não fazer sentido para uma empresa gastar mais recursos na segurança do que no próprio produto, por outro lado, fará menos sentido ainda gastar mais nas compensações por danos causados por falhas do que na melhoria das suas soluções [21].

De forma ampla, a motivação para o ataque a um sistema é essencialmente modificar o seu comportamento, seja para fazer com que este se comporte de maneira diferente para o qual foi projetado, seja para obter vantagem indevida de qualquer natureza na sua utilização ou até mesmo impedir o seu funcionamento. Com o avanço e a integração de novas tecnologias, os sistemas embarcados automotivos estão viabilizando novos modelos de negócios para a indústria, refletindo a grande competição existente no mercado, como também novas ameaças que podem ser exploradas pelos agressores.

Sistemas imobilizadores anti-furto estão presentes nos veículos há algum tempo e têm impacto direto na prevenção ao roubo. Estes sistemas são baseados em criptografia e também impactam no valor cobrado pelas companhias de seguro, e como consequência deste, no valor de revenda dos veículos, reputação da marca e também no volume de vendas [2]. A eventual ineficácia desses sistemas exemplifica como a segurança dos sistemas embarcados automotivos se relaciona com o mercado direta e indiretamente.

A evolução da eletrônica permitiu que as ECUs se tornassem cada vez mais complexas. Hoje é possível o uso de uma mesma ECU (*hardware*) para diversos modelos de veículos de uma marca, entregando funcionalidades diferentes (*software*) com base na categoria do veículo, seja um modelo de entrada, intermediário, luxo ou esportivo. Essa versatilidade permite a uma empresa reduzir seus custos tanto na fase de projeto, uma vez

que não necessita elaborar, desenvolver, testar e validar projetos distintos de ECUs, como também na complexidade de manter diversas linhas de produção ou montagem.

A atualização do *software* das ECUs também é uma possibilidade interessante para a indústria, pois permite que eventuais melhorias ou correções de falhas sejam detectadas e aplicadas em veículos que já se encontram em operação. O revés dessa situação reside no fato de que, uma vez violada a segurança de uma ECU, seja possível modificar o sistema e ter acesso a funcionalidades que não foram entregues para aquele modelo específico. A prática do *performance tuning* nas ECUs, consiste em modificar seu software de forma a alterar seu padrão ou condições de funcionando com o foco no aumento da performance, também é um problema [2] [11].

Alterações dessa natureza feitas por pessoas não autorizadas em sistemas como controle de injeção eletrônica de combustível, motor e transmissão modificam o padrão de funcionamento e comportamento do veículo como um todo e trazem como consequências o eventual desgaste de componentes com a redução acelerada de suas vidas úteis, alteração na emissão de poluentes, dinâmica veicular e dirigibilidade e segurança dos ocupantes.

Ao embarcar sistemas de entretenimento e informação nos veículos surge também a preocupação com a proteção desse conteúdo contra uso não autorizado (pirataria) e a privacidade dos dados dos usuários. A conectividade dos veículos com o mundo externo através de enlaces de rede sem-fio permite o consumo de mídia (áudio e vídeo), informações sobre navegação e serviços sob demanda baseados em geolocalização com possibilidade de contratação e pagamento *online*. Já existem vários modelos de negócios disponíveis no mercado e em 2004 mais de 50% dos veículos tipo *mini-van* vendidos nos EUA foram equipados com telas nos bancos traseiros [2]. Empresas que atuam no mercado consumidor Europeu, por conta da GDPR, agora precisam garantir a privacidade dos dados de seus usuários sob pena de graves implicações legais [24].

A segurança da informação nos sistemas embarcados automotivos impacta não somente nas empresas que fazem parte da indústria automotiva mas também nas companhias de seguro, empresas que produzem conteúdo digital para entretenimento e informação, além dos consumidores finais. Ao considerarmos as consequências da quebra da segurança nos sistemas, conforme apresentado no capítulo anterior, temos nesses exemplos todos os níveis anteriormente descritos (baixo, moderado e alto) que se traduzem em perdas financeiras, risco aos ocupantes além de implicações legais.

3.2 COMPLEXIDADE E SEGURANÇA

Em 2009 um Boing 787 que estava para ser lançado no mercado possuia cerca de 6,5 milhões de linhas de código, já um carro de luxo continha algo em torno de 100 milhões de linhas de código em seu *software* embarcado [25]. E a tendência não é diminuir,

pelo contrário: novas tecnologias, novas funcionalidades e serviços, mais conectividade e integração entre os sistemas, além da crescente quantidade de linhas de código nos softwares, os sistema embarcados automotivos contam também com centenas de processadores.

O avanço da tecnologia claramente nos traz diversas melhorias: processadores mais rápidos, com menor consumo de energia e custo de produção reduzido permitem por exemplo aplicar a criptografia em vários dispositivos embarcados. Mas como dito anteriormente, o aumento da complexidade necessariamente torna os sistemas menos seguros [21], essa é uma realidade fácil de compreender quando analisamos os sistemas embarcados automotivos individualmente e também dentro do seu contexto.

Em 2005 a Toyota convocou cerca de 160 mil clientes para um *recall* com objetivo de corrigir uma falha de *software* no modelo Prius que causava o desligamento do veículo. O tempo estimado no reparo era de 90 minutos por veículo [25]. Com essa informação é possível calcular o prejuízo financeiro, além do impacto causado a imagem da empresa que poderia ser ainda maior se a falha em questão tivesse sido explorada em um ataque ao sistema.

Ao pensar sobre a segurança no desenvolvimento de um sistema é importante ter em mente sua complexidade, ameaças e riscos, analisar de forma realista o que pode dar errado, que tipos de ataques o sistema está sujeito, quais as consequências destes ataques e qual a influência do ambiente externo, seja na interação com os outros sistemas ou o fator humano. Muitos ataques são bem sucedidos quando um desses pontos é negligenciado, como por exemplo o ataque do tipo *side channel* que será apresentado adiante e se baseia na manipulação física do ambiente externo.

Durante a fase de desenvolvimento do sistema existe a preocupação em atender os requisitos que implementam as funcionalidades para o qual aquele sistema em específico foi desenhado na fase de projeto, por exemplo: permitir ao motorista controlar a abertura e fechamento das portas do veículo através de rádio frequência (RFID), usando um dispositivo portátil que caiba no seu bolso e consuma pouca energia durante seu funcionamento. Ao mesmo tempo, é necessário se preocupar também que essa funcionalidade não comprometa a segurança do veículo, por exemplo: garantir que somente um disposito previamente configurado efetue esse controle no acesso ao veículo.

Assim como qualquer sistema computacional, cada sistema presente nos veículos (*software* e *hardware*) já traz consigo sua própria complexidade. Os sistemas embarcados automotivos são sistemas distribuídos que interagem entre si e também com o ambiente externo através de redes de comunicação, portanto, potencializando essa complexidade individual existente em cada um.

A medida que um *software* cresce e se torna mais complexo, a quantidade de linhas de código aumenta e com ela também o número de falhas (*bugs*) que trazem problemas

de performance e comportamentos inesperados [21]. Muitas dessas falhas podem também se traduzir em falhas de segurança com potencial para ser exploradas por um agressor, por exemplo: um estouro de pilha de memória com vazamento de dados ou um problema de concorrência por recursos do sistema. Toda essa complexidade será necessariamente transferida para a fase de testes do sistema, tornando esta uma difícil e crucial tarefa na gestão da segurança da informação.

Um número grande de interações entre os módulos de um sistema, através da troca de informações e contextos, torna mais difícil a manutenção da segurança, sendo necessário o desenho de uma boa arquitetura durante a fase de projeto que separe os diversos módulos de forma clara, concisa e que favoreça a independência destes fornecendo o acoplamento adequado. Uma boa modularização através da redução da complexidade e acoplamento aumenta a testabilidade do sistema e favorece a segurança sem a necessidade de eliminar funcionalidades importantes [21].

Em geral, uma boa parte dos *bugs* de performance são encontrados e corrigidos durante a fase de teste dos sistemas, mas as falhas de segurança podem seguir ocultas, pois muitas vezes surgem a partir da interação entre os diferentes módulos do sistema, e principalmente, do uso incomum para o qual casos de teste não foram previstos e muitas vezes também fora do ambiente para o qual foram projetados para operar. Testar se uma informação foi criptografada com sucesso, trazendo seu conteúdo cifrado e ilegível, e depois descriptografada trazendo seu conteúdo original não é suficiente para dizer se aquele mecanismo de criptografia é realmente seguro [21].

Testes de segurança tem foco específico e procuram manipular o sistema de forma deliberada com objetivo de provocar efeitos inesperados. Em 2010 um grupo de pesquisadores conseguiu explorar uma vulnerabilidade na comunicação sem-fio de sensores de medição de pressão de pneus (TPMS), injetando dados maliciosos que foram então enviados através do barramento CAN na rede de comunicação veicular para uma ECU. Com este ataque, foi possível não só adulterar informações que eram transmitidas para a ECU como também rastrear o veículo em questão, violando não somente a integridade como a privacidade do sistema [26] [27]. Importante frisar que hoje esses sensores são obrigatórios em veículos novos, por força da legislação, nos Estados Unidos e União Européia.

Esse exemplo demonstra a visão da segurança de sistemas ao lidar com as complexidades inerentes a própria natureza do sistema: garantir que este será utilizado tão somente conforme desenhado e de acordo com as premissas da confidencialidade, integridade e disponibilidade. A eficácia na segurança dos sistemas depende dos seguintes fatores [17]:

a) Política: qual é o objetivo a ser alcançado.

b) Ferramentas: soluções e mecanismos que serão utilizados para implementar garantir a política de segurança como controle de acesso, cifras criptográficas,

dispositivos anti fraude para *hardware*.

c) Garantias: quanta confiança é possível depositar em cada ferramenta.

d) Incentivos: motivações tanto por parte das pessoas envolvidas em manter o sistema seguro como também daqueles interessados em burlar a segurança do sistema.

Na prática e no mundo real isso é muito mais complexo e muitos sistemas falham ao proteger os elementos errados ou proteger os elementos corretos da maneira errada [21].

3.3 SUPERFÍCIES DE ATAQUES E MODELO DE AMEAÇAS

As demandas para a indústria automotiva são também consequência da evolução da própria tecnologia: veículos mais eficientes, menos poluentes, mais seguros, mais confortáveis e conectados com outras ferramentas que já temos a disposição. Claro que existem políticas ou legislações específicas que por vezes orientam esses avanços, além disso, muitas vezes é necessário aguardar até que certa tecnologia evolua até o ponto de ser aplicada em determinado contexto, por exemplo: o tamanho reduzido e consumo energético de um processador, a precisão de um sensor ou a eficiência de um motor elétrico ou bateria.

A segurança da informação só existe dentro de um contexto, e compreender o contexto no qual se encontra o sistema em questão é mais importante do que a própria tecnologia empregada [21]. O contexto vai definir até onde a segurança deve ir: o que proteger, como proteger e em detrimento de quais aspectos ou características do sistema. Tempo, custos, funcionalidades, a experiência do usuário final com o sistema e até a competição no mercado podem ser alguns desses aspectos a ser considerados.

Já as ameaças, essas não mudam muito mas não deixam de acompanhar as evoluções tecnológicas, se adequando também ao mesmo contexto: basta que exista uma vulnerabilidade, a motivação e uma oportunidade para que exista uma ameaça. Se antes um agressor necessitava de acesso físico e direto a um sistema computacional, hoje é possível atacar um sistema que está do outro lado do mundo, e isso certamente se aplica aos sistemas embarcados automotivos. Eis um bom exemplo: recentemente um proprietário de um carro Testa publicou um vídeo demonstrando o controle remoto através da Internet que lhe permitiu abrir a mala do seu veículo para um entregador da Amazon deixar sua encomenda quando não estava em casa [28].

Pensar sobre quais ameaças existem ao sistema é o primeiro passo na sua segurança. Elaborar um modelo que leve em consideração as reais ameaças as quais o sistema está exposto nos permite delimitar uma superfície de ataques e consequentemente saber o quão exposto se encontra o sistema. Dessa forma será possível desenvolver as contramedidas necessárias para cada risco identificado [11] [21].

Proteger um sistema contra um risco que está fora de sua realidade pode ser economicamente inviável, assim como ignorar um risco real mas improvável pode comprometer todo o sistema, porque essa vulnerabilidade só precisará ser explorada uma única vez. A superfície de ataques diz respeito a todas as possíveis formas de se atacar o sistema, sem levar tanto em consideração como atacar mas sim todas as entradas disponíveis naquele sistema, quanto maior a superfície, mais exposto está o sistema [11].

Todas as possíveis entradas de dados e interações nos sistemas embarcados automotivos serão o ponto de partida para o levantamento da superfície de ataques do veículo: tipos de sinais recebidos, se existem dispositivos físicos de entrada como teclados, telas sensíveis ao toque, portas USB ou de serviço de diagnóstico [11]. Considerando essas entradas é possível elaborar um diagrama inicial que descreve suas relações com o veículo, levando em consideração se é uma entrada externa ou interna ao veículo, conforme a figura 7. Os retangulos representam as entradas e os círculos são unidades com maior grau de complexidade.

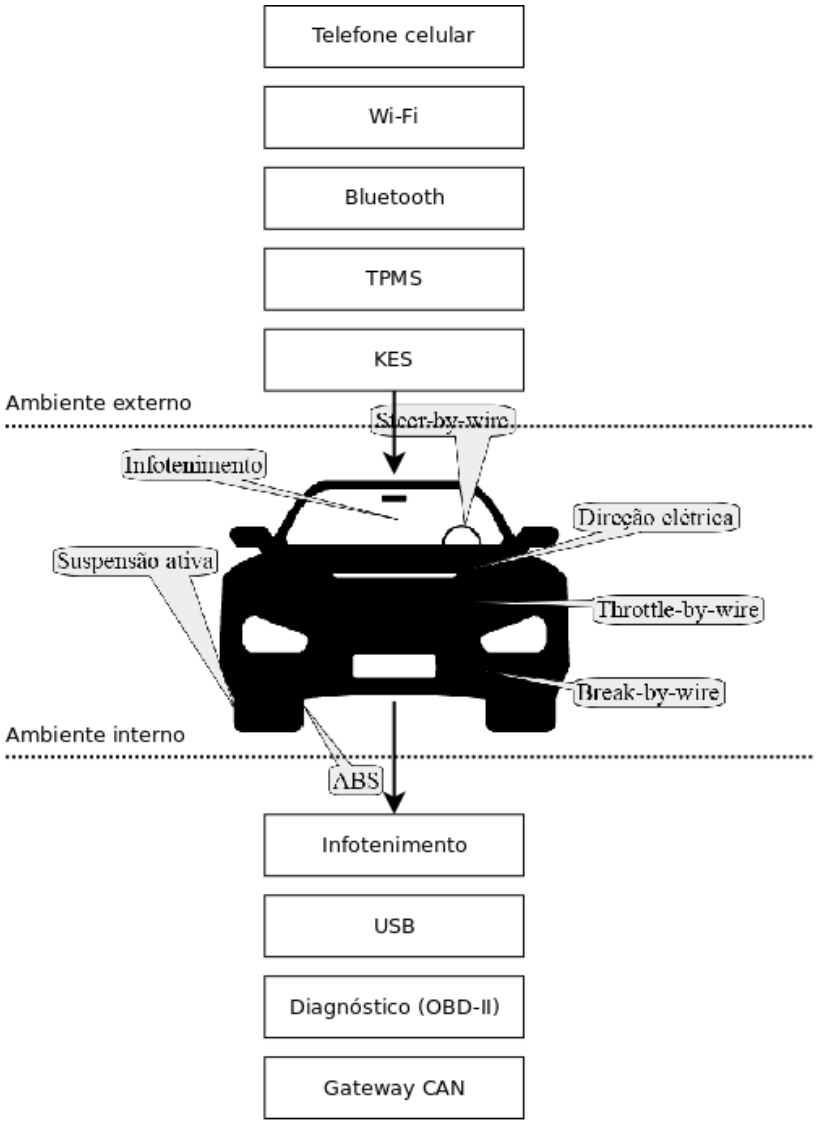
Ao aprofundarmos a análise é possível visualizar em maior detalhe as interações, assim como surgem também novos subsistemas como entretenimento e informação, imobilizador (anti-furto) e monitoramento de pressão nos pneus, como vemos na figura 8. Estes interagem diretamente com as ECUs e estão portanto numa região mais próxima e mais sensível na segurança do sistema automotivo. Quanto mais próxima e confiável é a relação entre os sistemas, mais perigosa.

O próximo passo é analisar cada subsistema individualmente e suas interações, por exemplo o sistema de entretenimento e informação apresentado na figura 9. Consideremos um sistema IVI baseado no sistema operacional Linux que oferece diversas funcionalidades para o usuário e conexão muitas vezes direta com a rede de comunicação interna do veículo. Aqueles componentes mais próximos, que interagem diretamente com o *kernel* do Linux, representam maior risco se exploradas vulnerabilidades na sua segurança, pois podem ignorar outros mecanismos de segurança como controles de acesso aos quais outros elementos estão sujeitos [11]. Nesse exemplo, o canal de comunicação com telefone celular oferece maior risco uma vez que interage diretamente com um módulo mais interno do sistema operacional, executado em *kernel space*, diferentemente do módulo Wi-Fi que é executado em *user space*.

Sistemas de entretenimento e informação baseados em Linux são comuns hoje na indústria automotiva [29] e trazem em conjunto outros subsistemas como udev (responsável pela gestão de dispositivos conectados ao sistema), HSI (interface de comunicação com telefones celulares) e Kvaser (interface de comunicação com *transceiver* CAN), e assim como as versões para computadores pessoais, estes também podem apresentar vulnerabilidades a ser exploradas.

A partir da superfície de ataques é possível elaborar um modelo de ameaças que

Figura 7 – Entradas externas e internas para superfície de ataques em um sistema embarcado automotivo

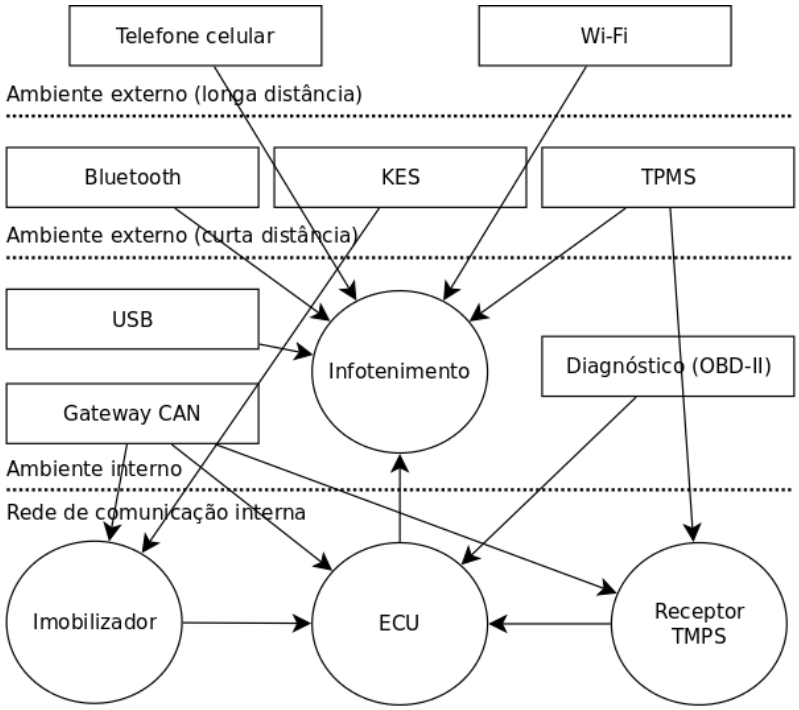


Fonte: Adaptado de [11].

levará em consideração cada ameça e seus principais aspectos: quão fácil é descobrir a falha, facilidade de reprodução da falha, facilidade de exploração da falha, potencial de produzir dano e quantidade de usuários afetados [11].

Essas análises em geral precisam ser feitas ao longo dos ciclos de projeto e desenvolvimento do sistemas e dependem de constante atualização, demandam tempo e têm impacto no custo do projeto. É importante considerar possibilidades que estão além do óbvio, a criatividade de um agressor ao pensar sobre como manipular um sistema para obter sucesso ao procurar ou explorar uma vulnerabilidade sempre será uma vantagem sobre aqueles que projetaram o sistema. A partir da figura 7 começamos a elencar as possíveis ameaças [11]:

Figura 8 – Entradas e interações entre os subsistemas



Fonte: Adaptado de [11].

a) Acessar remotamente o veículo.

b) Desligar o veículo.

c) Violar a privacidade dos usuários.

d) Destrancar o veículo.

e) Rastrear o veículo.

f) Desabilitar mecanismos que impactam na segurança dos usuários.

g) Instalar um *software* mal intencionado no veículo (*malware*, *ransomware*).

Ao focar nas entradas e interações entre os subsistemas apresentadas na figura 8, teremos as seguintes possibilidades [11]:

Telefone celular:

a) Acessar remotamente o veículo.

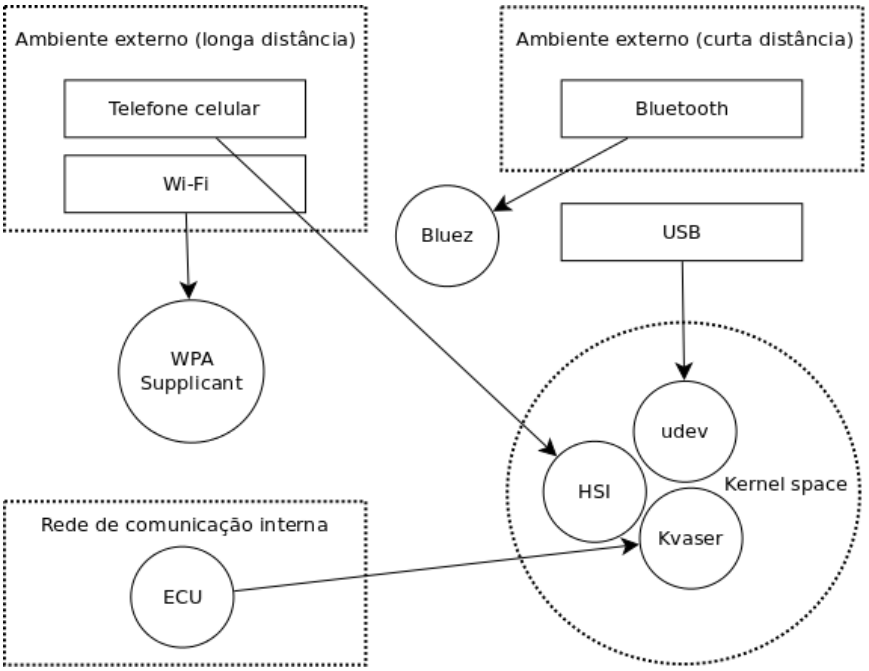
b) Explorar uma vulnerabilidade no sistema de infotenimento que gerencia a agenda de contatos e o recebimento de ligações.

c) Conectar remotamente a um serviço de suporte e diagnóstico como OnStar.

d) Rastrear o veículo.

Conexão Wi-Fi:

Figura 9 – Detalhe da análise do sistema de entretenimento e informação



Fonte: Adaptado de [11].

a) Acessar remotamente o veículo.

b) Explorar uma vulnerabilidade no sistema de infotenimento que gerencia conexões.

c) Instalar um *software* mal intencionado no sistema de infotenimento.

d) Quebrar a senha da conexão Wi-Fi.

e) Simular uma conexão de serviço de manutenção com o veículo.

f) Monitorar a comunicação do veículo através da rede Wi-Fi.

Sistema de acesso sem chave (*Keyless Entry System*, KES):

a) Enviar requisições com pacotes corrompidos com objetivo de colocar o imobilizador do sistema anti-furto em estado inoperante, ataque de negação de serviço (*Denial of Service*, DOS).

b) Enviar alto volume de requisições com objetivo de drenar a bateria do veículo através do imobilizador.

c) Capturar informações sobre a chave criptográfica durante o *handshake*.

d) Quebrar a chave criptográfica através de ataque de força bruta.

e) Clonar as informações da chave de acesso.

f) Embaralhar e interferir no sinal do chaveiro.

g) Drenar a bateria do chaveiro.

Sistema de monitoramento da pressão dos pneus (TPMS):

a) Enviar requisições com pacotes corrompidos que prejudiquem a operação da ECU.

b) Enviar informações incorretas para a ECU que disparem alertas relacionados a condição de operação do veículo.

c) Rastrear o veículo através do código identificador do sistema.

Sistema de infotenimento:

a) Forçar o sistema a executar em modo de manutenção ou *debug*.

b) Manipular configurações ou informações de manutenção.

c) Instalar *software* mal intencionado.

d) Acessar a rede de comunicação interna do veículo através de *software* mal intencionado.

e) Violar a privacidade do usuário através do monitoramento das informações.

f) Manipular ou forjar informações que serão exibidas para o usuário.

Portas USB:

a) Instalar *software* mal intencionado ou modificar o sistema de infotenimento.

b) Explorar uma vulnerabilidade no suporte USB do sistema de infotenimento para conseguir acesso privilegiado.

c) Danificar fisicamente a porta USB e o sistema de infotenimento.

Conexão Bluetooth:

a) Acessar remotamente o veículo.

b) Instalar *software* mal intencionado ou modificar o sistema de infotenimento.

c) Explorar uma vulnerabilidade no suporte Bluetooth do sistema de infotenimento para conseguir acesso privilegiado.

d) Enviar informações corrompidas, por exemplo catálogo de contatos, para o sistema de infotenimento com objetivo de modificar o sistema.

Gateway CAN:

a) Acessar a rede de comunicação interna do veículo através do ambiente externo.

b) Enviar pacotes corrompidos para alguma ECU através da rede de comunicação.

c) Manipular informações de diagnóstico do veículo.

d) Causar mal funcionamento em alguma ECU do veículo.

Analisando o sistema de entretenimento e informação e seus componentes apresentados na figura 9 é possível identificar ameaças mais específicas. Estas informações serão a base para a construção do modelo de ameaças:

Sistema de suporte ao Bluetooth, Bluez:

a) Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques.

b) Versões antigas ou desatualizadas podem não oferecer suporte apropriado a criptografia.

c) Versões antigas ou desatualizadas podem utilizar senhas padrão, por exemplo: 0000.

Sistema de suporte ao Wi-Fi, WPA Supplicant:

a) Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques.

b) Versões antigas ou desatualizadas podem não forçar o uso de criptografia mais segura (WPA2).

c) Podem ser induzidos a conectar em pontos de acesso mal intencionados.

d) Podem vazar informação via interface de rede (BSSID).

Sistema de suporte a telefones celulares, HSI:

a) Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques.

b) Podem ser suscetíveis a inserção de pacotes maliciosos contendo comandos durante a comunicação serial, ataque do tipo *man-in-the-middle*.

Sistema de suporte a dispositivos USB, Udev:

a) Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques.

b) Pode permitir o uso de dispositivos que não foram concebidos para o uso, como por exemplo teclado USB, que poderá ser utilizado para manipular o sistema.

Sistema de suporte a *transceivers* CAN, Kvaser:

a) Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques.

b) Pode permitir o uso de *firmware* contendo código mal intencionado.

Existem várias metodologias para elaboração de modelos de ameaças. Sistemas como ISO 26262 são utilizados pela industria automotiva mas com foco somente na segurança dos ocupantes e não dos sistemas embarcados automotivos. O modelo DREAD permite realizar a análise qualitativa dos riscos identificados [30], sendo portanto mais adequado ao cenário proposto.

O sistema DREAD leva em consideração e pontua os seguintes aspectos [11]:

a) *Damage potencial*: qual o tamanho do dano causado?

b) *Reproducibility*: quão fácil é reproduzir?

c) *Exploitability*: quão fácil é explorar?

d) *Affected users*: quantos usuários serão afetados?

e) *Discoverability*: quão fácil é descobrir a falha?

Seguimos na tabela 2 o mesmo raciocínio apresentado no capítulo anterior, onde mensuramos o impacto sobre as organizações e os indivíduos na quebra da segurança nos sistemas.

Tabela 2 – Pontuação DREAD para modelo de ameaças

Categoria	**Alto (3)**	**Moderado (2)**	**Baixo (1)**
Dano	Prejudicar o sistema como um todo dando acesso privilegiado e irrestrito	Vazar informação sensível	Vazar informação trivial
Reprodutibilidade	Sempre possível	Possível durante circunstâncias específicas	Difícil mesmo com informações específicas
Explorabilidade	Qualquer agressor	Necessita de conhecimento específico	Necessita de conhecimento profundo e muito especializado
Alcance	Afeta todos os usuários incluindo configuração padrão de fábrica	Afeta usuários específicos	Afeta poucos usuários, geralmente em configurações específicas
Descoberta	Encontrado facilmente	Encontrado em parte específica e pouco acessível	Obscura e nada acessível

Fonte: Adaptado de [11].

A partir da pontuação alcançada pela análise em questão é possível aplicar a classificação de riscos e mensurar seu impacto, conforme a tabela 3.

Aplicando o modelo DREAD ao sistema de suporte a telefones celulares (HSI) e levando em consideração a superfície de ataques apresentada anteriormente teremos o seguinte resultado, conforme a tabela 4.

Tabela 3 – Análise da pontuação DREAD para modelo de ameaças

Total de pontos	Impacto
5-7	Baixo
8-11	Moderado
12-15	Alto

Fonte: Adaptado de [11].

Tabela 4 – Modelo de ameaças para o sistema de suporte a telefones celulares (HSI)

Ameaça	D	R	E	A	D	Total	Impacto
Versões antigas ou desatualizadas podem conter vulnerabilidades passíveis de ataques	3	3	2	3	3	14	Alto
Podem ser suscetíveis a inserção de pacotes maliciosos contendo comandos durante a comunicação serial, ataque do tipo *man-in-the-middle*	2	2	2	3	3	12	Alto

Fonte: Adaptado de [11].

Seguindo o processo apresentado no capítulo anterior, agora que as ameças foram identificadas, compreendidas e categorizadas, temos a possibilidade de definir as estratégias para mitigá-las. No caso específico do sistema HSI, está claro que uma versão antiga ou desatualizada do *software* oferece grande risco ao sistema de infotenimento, logo, é necessário pensar em qual ou quais contramedidas serão adotadas. As tabelas 5 e 6 apresentam as contramedidas para cada ameaça encontrada no sistema HSI.

Tabela 5 – Contramedidas para execução de código malicioso no sistema de suporte a telefones celulares (HSI)

Ameaça	Execução de código malicioso em *kernel space*
Risco	Alto
Ataque	Explorar vulnerabilidade em versão antiga do software HSI
Contramedida	Atualizar o *kernel* e seus módulos para última versão disponível

Fonte: Adaptado de [11].

Tabela 6 – Contramedidas para ataque *man-in-the-middle* no sistema de suporte a telefones celulares (HSI)

Ameaça	Injeção de comandos através da comunicação serial
Risco	Alto
Ataque	Interceptar comunicação serial através do módulo HSI
Contramedida	Utilizar criptografia na comunicação

Fonte: Adaptado de [11].

3.4 EXEMPLOS DE ATAQUES A SEGURANÇA

Vimos até aqui como a evolução da tecnologia nos sistemas embarcados automotivos, motivada e impulsionada pelas constantes demandas do mercado, impactam na segurança desses sistemas, além das consequências desse impacto para todos os envolvidos: fabricantes

e montadoras, fornecedores de soluções diversas e prestadores de serviços, companhias de seguro, governo e claro, os consumidores.

O CERT é uma divisão de pesquisa com foco em *cyber* segurança. Criada nos Estados Unidos em 1988 pela DARPA (*Defense Advanced Research Projects Agency*), o CERT é parte do SEI (*Software Engineering Institute*) da Universidade Carnegie Mellon e colabora com a indústria, academia e governo na pesquisa, análise e resposta a incidentes de segurança da informação, interagindo com desenvolvedores de *hardware* e *software* [31].

O número sempre crescente de vulnerabilidades reportadas ao CERT confirma a afirmação anteriormente feita de que a complexidade é a pior inimiga da segurança. Essas vulnerabilidades são resultado do desenho e implementação inadequados, além de práticas de desenvolvimento que não focam em evitar problemas de implementação que poderão resultar em falhas. Ao descobrir uma falha, a empresa responsável pode produzir uma correção (*patch*), mas mesmo esse processo pode ser bastante complexo e levar muito tempo até que todos os sistemas vulneráveis sejam corrigidos [32].

O resultado desse cenário é que muitos sistemas seguirão desprotegidos e suscetíveis a ataques, e apesar da resposta rápida e eficiência na correção de uma vulnerabilidade ser importante, deve-se pensar e agir no sentido de produzir sistemas de qualidade. Análises do CERT mostram que a maior parte dos incidentes de segurança estão relacionados a *trojans*, ataques de engenharia social e exploração de vulnerabilidades em *softwares* por conta de falhas específicas, desenho, configurações e interações inadequadas entre sistemas [32], e tudo isso potencializado pela conectividade através das redes de computadores e a Internet.

Em 2006 o *W32.Blaster.Worm* infectou cerca de 8 milhões de sistemas em todo o mundo. Em 24 horas, 336 mil computadores foram afetados com um pico de 100 mil sistemas infectados por hora. Isso aconteceu 26 dias após a liberação de uma correção para a falha descoberta na implementação do software RPC (*Remote Procedure Call*) que permite que sistemas remotos se comuniquem entre si para a execução de rotinas. A vulnerabilidade explorada nessa funcionalidade extremamente útil para comunicação inter-processos afetou todas as versões dos sistemas operacionais Windows na época, causando prejuízos estimados na ordem de 500 milhões de dólares com a perda de produtividade e indisponibilidade de sistemas e redes de comunicação [32].

Uma vez que os riscos associados a insegurança dos sistemas pode ser avaliada com base em fatores históricos e o potencial existente para ataques futuros [32], e por todo o exposto até aqui, é possível afirmar que não estamos distantes de cenários como esse quando consideramos os sistemas embarcados automotivos.

Já vimos que muitos sistemas embarcados automotivos se comunicam através de sinais sem-fio. Geralmente esses sistemas empregam como única medida de segurança o uso

de sinais de curta distância, na tentativa de garantir que somente o proprietário estando próximo do veículo e de posse do chaveiro que contém a chave de acesso será capaz de enviar esses sinais para a ECU que controla o imobilizador anti-furto do veículo.

Os sistemas mais modernos utilizam um método de rotacionamento de códigos de acesso e pergunta e resposta entre o chaveiro, que envia o sinal e o receptor, que controla o imobilizador, o que previne que o código trocado entre eles seja memorizado e replicado permitindo acesso não autorizado. O sistema de pergunta e resposta exige que o sistema realize cálculos e por esse motivo consome mais energia da bateria, ao mesmo tempo aumentando a potência e o alcance do sinal de comunicação [11].

Uma forma de ataque é através da geração e injeção de ruídos na mesma faixa de frequência que o sistema receptor está operando. Essa faixa geralmente inclui um espaço extra não utilizado, e o ruído injetado pode impedir o receptor de rotacionar o código que está esperando do chaveiro emissor, dando tempo a pessoa que está atacando de analisar e replicar a sequência correta a ser enviada para o veículo. No momento em que o usuário do veículo emite um sinal válido através do seu chaveiro, esse sinal é capturado e salvo, e no momento em que o usuário não estiver mais presente, o atacante poderá usar o código salvo para desbloquear o veículo [11].

Esse ataque já foi estudado, demonstrado [33] e amplamente noticiado, e hoje existem disponíveis no mercado dispositivos prontos que tornam simples a exploração dessa vulnerabilidade em diversas marcas de veículos [34] [35]. Técnicas e ferramentas adequadas baseadas em criptografia para a comunicação desses sistemas poderiam ser aplicadas para impedir esse ataque conhecido como *man-in-the-middle* [36], que tem impacto econômico direto tanto no valor do seguro como no volume de vendas dos veículos.

Ainda considerando os sistemas embarcados que se comunicam através de enlaces sem-fio, através do sistema de monitoramento de pressão de pneus (TPMS) já apresentado, é possível rastrear um veículo enviando sinais falsos de ativação para os sensores que possuem identificadores únicos, violando assim a privacidade de seu usuário. Esses sistemas também são vulneráveis ao envio de sinais de eventos falsos através de pacotes forjados que podem sobrecarregar ao ponto de tornar inoperante uma ECU [11] [26] [27], um exemplo de ataque conhecido como negação de serviço (DOS) com grau de complexidade e custo relativamente simples de ser executado.

O ataque ao sistema de entretenimento e informação dos veículos também apresenta baixa complexidade e custo em sua execução. Através do dispositivo conhecido como *USB kill* é possível gerar uma corrente elétrica que será descarregada quando conectado a uma entrada USB como as disponíveis nos consoles IVI, destruindo o sistema. Esse dispositivo pode ser comprado livremente e custa cerca de 60 dólares [37] [38]. É possível também instalar ou promover alterações de *software* não previstas pelo fabricante utilizando a mesma entrada USB ou até mesmo a unidade de CD presente no console. Essas alterações

podem permitir a violação de direitos (pirataria) relacionada ao conteúdo digital de um determinado fornecedor, como por exemplo serviço de mapas ou entretenimento [2].

A proteção contra ataques ao *hardware*, seja adulteração ou destruição, possui componentes de complexidade e imprevisibilidade relacionadas ao ambiente no qual aquele equipamento opera. Ataques do tipo *side channel* apresentam maior grau de complexidade e especialização na sua execução e têm como objetivo por exemplo quebrar a criptografia empregada em diversos sistemas embarcados automotivos.

Ataques do tipo *side channel* consistem em monitorar ou interferir na operação do *hardware* como tempo de execução, consumo de energia ou emissões eletromagnéticas, com objetivo de comprometer o algorítmo criptográfico implementado neste. Essas são técnicas mais sofisticadas que envolvem engenharia reversa e geralmente as contramedidas estão relacionadas a descaracterizar o funcionamento do sistema, por exemplo, tornando a execução de um algorítmo criptográfico invariante no tempo, gerando ruído adicional para dificultar a identificação de um padrão de emissão eletromagnética ou empregando transistores com consumo de energia constante [2]. Claro que todas essas contramedidas têm um custo seja na perda de performance na execução do *software* ou no aumento do consumo de energia do *hardware*, e faz parte do desafio da engenharia da segurança lidar com esses aspectos.

Não é incomum encontrar imobilizadores que utilizam sistemas de criptografia proprietários e que empregam a segurança baseada na obscuridade. Conforme já discutido, esse tipo de segurança está fadada ao fracasso uma vez que é praticamente impossível uma empresa com a natural limitação de profissionais e tempo, dedicar os mesmos esforços comparado a toda uma comunidade especilizada ao testar um novo sistema criptográfico [21]. Por esse motivo são vários os casos onde algorítmos criptográficos que foram quebrados e não é incomum também que ainda assim, essas tecnologias continuem presentes nos veículos. A tabela 7 apresenta alguns exemplos.

Tabela 7 – Algorítmos criptográficos proprietários quebrados

Nome	**Fabricante**	**Veículos**	**Status**
EM Micro Megamos	Volkswagen/Thales	Audi, Bentley, Lamborghini, Porsche	Detalhes da metologia de ataque foram censurados por força da lei [23]
Hitag 2	Philips/NXP	Audi, Bentley, BMW, Chrysler, Land Rover, Mercedes Benz, Porsche, Saab, Volkswagen	Quebrado através de ataque de força bruta e dicionário
DST-40	Texas Instruments	Ford, Lincon, Mercury, Nissan, Toyota	Qubrado através de ataque de força bruta utilizando FPGA [39]

Fonte: Adaptado de [11].

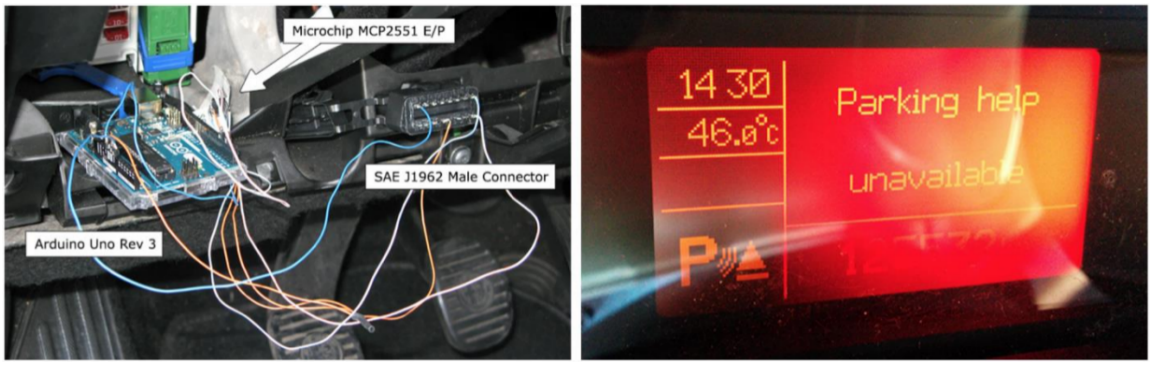
Em 2011 a Atmel lançou um protocolo criptográfico de código aberto para imobilizadores, *Open Source Immobilizer Protocol Stack*, tornando este amplamente disponível para análise de toda a comunidade especializada bem como a indústria [40]. Já em 2012 uma análise desse protocolo foi publicada identificando potenciais vulnerabilidades e propondo para cada uma destas as contramedidas necessárias [41]. Esse é um dos benefícios diretos ao se empregar sistemas onde sua implementação é conhecida e mais importante, pode ser testada. Até o presente momento não foram encontradas publicações que sugerem que esse protocolo tenha sido quebrado.

Recentemente foi publicada uma falha que afeta a grande maioria dos veículos modernos, essa falha na verdade está relacionada com o desenho do protocolo CAN e é considerada irreparável [42]. As mensagens CAN assim como os erros são chamados de *frames* e o ataque consiste em explorar como o protocolo lida com os erros. Os erros surgem quando um dispositivo na rede de comunicação lê um valor que não corresponde ao esperado, nesse momento, o dispositivo envia uma mensagem no barramento solicitando o reenvio e notificando aos outros dispositivos que ignorem aquele que será enviado novamente.

Acontece que, se por qualquer motivo um volume alto de mensagens de erro chegar ao barramento, pelo próprio desenho do protocolo, ele entra em um estado de desligamento impedindo que qualquer dispositivo leia ou escreva mensagens no barramento. Essa é uma estratégia útil para isolar um segmento com mal funcionamento e estratégias similares de proteção como *bus guardian* são implementadas em outros protocolos de comunicação como o *FlexRay* [10].

O ataque consiste em explorar essa característica do protocolo, onde um agressor gera um alto volume de erros no barramento forçando-o a entrar no estado de desligamento, outro exemplo de negação de serviço (DOS) com consequências muito maiores dado o grau de criticidade no uso das redes de comunicação CAN. Essa falha pode ser apenas mitigada e não completamente eliminada a não ser por um completo redesenho do protocolo. A figura 10 apresenta um exemplo onde o sistema de assistência de estacionamento foi danificado através desse ataque, executado com sucesso utilizando equipamento pouco especializado, de baixo custo (cerca de 30 dólares) e na ocasião sequer necessitou escrever mensagens no barramento para causar a falha [42].

Figura 10 – Ataque a rede e protoloco de comunicação CAN



Fonte: Adaptado de [42].

4 CONCLUSÃO

A segurança da informação deve ser vista como um processo que se relaciona com os negócios e as pessoas, e não com a tecnologia. A tecnologia é somente a ferramenta que auxilia na solução dos problemas, mas que sempre exigirá a responsabilidade dos envolvidos [21].

A alta competitividade na indústria traz a demanda por funcionalidades em um curto espaço de tempo, muitas vezes dando menor importância à qualidade ou à segurança dos sistemas durante seus ciclos de projeto, desenvolvimento e testes, ainda muito longe de chegar ao mercado consumidor. É necessário que existam incentivos, seja através do próprio mercado consumidor ou por força da legislação, para que as empresas priorizem a qualidade e a segurança dos seus produtos.

Nesse cenário, a segurança da informação pode ser vista também como uma espécie de seguro para as empresas, uma vez que o custo do investimento na segurança dos sistemas poderá vir a ser menor do que arcar com as consequências por eventuais falhas de segurança, sejam estas prejuízos financeiros diretos ou de sua imagem junto aos consumidores.

O aumento da complexidade, conectividade e a popularização dos sistemas embarcados automotivos traz consigo também novas oportunidades para que agressores em potencial tentem modificar esses sistemas. Conforme apresentado neste trabalho, é difícil prever o resultado da exploração de uma vulnerabilidade em um sistema por parte de um agressor, isso faz da segurança da informação um trabalho de responsabilidade e atenção permanente por parte das empresas e, mais do que isso, exige foco em ações que objetivem a qualidade e a segurança dos sistemas durante os ciclos de projeto, desenvolvimento e testes. O balanceamento entre segurança, usabilidade e performance virá como resultado das escolhas ainda durante a fase de desenho do projeto.

Os exemplos apresentados de vulnerabilidades existentes, bem como de ataques executados contra sistemas hoje disponíveis no mercado, mostram que essa é uma preocupação real, e entender o problema é crucial para aplicar com sucesso a tecnologia como ferramenta na sua solução.

REFERÊNCIAS

1 VALVANO, J. W. *Embedded Systems: Real-Time Operating Systems for ARM Cortex-M Microcontrollers Volume 3*. [S.l.: s.n.], 2014. Citado 3 vezes nas páginas 13, 15 e 17.

2 LEMKE, K.; PAAR, C.; WOLF, e. M. *Embedded Security in Cars: Securing Current and Future Automotive IT Applications*. New York: Springer, 2006. Citado 7 vezes nas páginas 13, 16, 28, 29, 30, 31 e 45.

3 WILWERT, C. et al. *Design of Automotive X-by-Wire Systems*. 2005. Disponível em: <http://nicolas.navet.eu/publications.html>. Acesso em: 15 nov. 2018. Citado 3 vezes nas páginas 13, 16 e 17.

4 SANTOS, M. M. D. *Redes de Comunicação Automotiva: Características, Tecnologias e Aplicações*. São Paulo: Érica, 2010. Citado 6 vezes nas páginas 13, 17, 19, 21, 22 e 23.

5 NATIONAL INSTRUMENTS. *Building Flexible, Cost-Effective ECU Test Systems*. 2014. Disponível em: <http://www.ni.com/white-paper/3064/en/>. Acesso em: 15 nov. 2018. Citado na página 18.

6 DIJK, L. van. *Future Vehicle Networks and ECUs*: Architecture and technology considerations. 2017. Disponível em: <https://www.nxp.com/products/analog/interfaces/in-vehicle-network/networking-innovation:NETWORKING-INNOVATION>. Acesso em: 15 nov. 2018. Citado na página 17.

7 SHANNON, C. E. *A Mathematical Theory of Communication*. 1948. Disponível em: <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 18 e 19.

8 ERICKSON, J. *Hacking The Art Of Exploitation*. 2. ed. San Francisco: No Starch Press, 2008. Citado na página 19.

9 KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet*: Uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006. Citado 2 vezes nas páginas 19 e 20.

10 NAVET, N.; SIMONOT-LION, F. *In-vehicle Communication Networks*: A historical perspective and review. 2013. Disponível em: <http://nicolas.navet.eu/publications.html>. Acesso em: 15 nov. 2018. Citado 3 vezes nas páginas 21, 22 e 46.

11 SMITH, C. *The Car Hacker's Handbook*: A guide for the penetration tester. San Francisco: No Starch Press, 2016. Citado 13 vezes nas páginas 22, 29, 30, 31, 34, 35, 36, 37, 38, 41, 42, 44 e 45.

12 NAVET, N.; SIMONOT-LION, F. *Trends in Automotive Communication Systems*. 2008. Disponível em: <http://nicolas.navet.eu/publications.html>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 22 e 23.

13 NATIONAL INSTRUMENTS. *FlexRay Automotive Communication Bus Overview*. 2016. Disponível em: <http://www.ni.com/white-paper/3352/en/>. Acesso em: 15 nov. 2018. Citado na página 23.

14 ROGERSON, S. *Vehicle Networking Opportunities*. 2016. Disponível em: <https://vehicle-electronics.biz/content/vehicle-networking-opportunities>. Acesso em: 15 nov. 2018. Citado na página 23.

15 TI SAFE SEGURANÇA DA INFORMAÇÃO. *Curso de Formação de Analista de Segurança: Gestão da Segurança da Informação*. 2008. Citado 4 vezes nas páginas 23, 25, 26 e 29.

16 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. *An Introduction to Computer Security: The NIST Handbook*. 1995. Citado na página 24.

17 ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2. ed. Indianapolis: Wiley, 2008. Citado 4 vezes nas páginas 24, 25, 26 e 33.

18 REGER, L. *The Architecture for Autonomous Driving*. 2017. Disponível em: <https://www.nxp.com/applications/solutions/automotive/driver-replacement: ADAS-AND-AUTONOMOUS-DRIVING>. Acesso em: 15 nov. 2018. Citado na página 24.

19 STALLINGS, W. *Criptografia e Segurança de Redes: Princípios e Práticas*. 6. ed. São Paulo: Pearson, 2015. Citado 2 vezes nas páginas 25 e 26.

20 AMBLER, S. W. *Security Threat Models: An Agile Introduction*. 2007. Disponível em: <http://agilemodeling.com/artifacts/securityThreatModel.htm>. Acesso em: 15 nov. 2018. Citado na página 27.

21 SCHNEIER, B. *Secrets And Lies: Digital Security In A Networked World*. Indianapolis: Wiley, 2004. Citado 8 vezes nas páginas 28, 29, 30, 32, 33, 34, 45 e 48.

22 RUSSELL HOTTEN. *Volkswagen: The scandal explained*. 2015. Disponível em: <https://www.bbc.com/news/business-34324772>. Acesso em: 15 nov. 2018. Citado na página 29.

23 BRITISH AND IRISH LEGAL INFORMATION INSTITUTE. *Volkswagen Aktiengesellschaft v Garcia & Ors 2013 EWHC 1832 Ch*. 2013. Disponível em: <http://www.bailii.org/ew/cases/EWHC/Ch/2013/1832.html>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 30 e 45.

24 FOXX, C. *Google and Facebook accused of breaking GDPR laws*. 2018. Disponível em: <https://www.bbc.com/news/technology-44252327>. Acesso em: 15 nov. 2018. Citado na página 31.

25 CHARETTE, R. N. *This Car Runs on Code*. 2009. Disponível em: <https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 31 e 32.

26 SCHNEIER, B. *Hacking Cars Through Wireless Tire-Pressure Sensors*. 2010. Disponível em: <https://www.schneier.com/blog/archives/2010/08/hacking_cars_th.html>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 33 e 44.

27 ROUF, I. et al. *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*. 2010. Disponível em: <http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 33 e 44.

28 DRON, W. *A Tesla Owner Wasn't at Home to Receive His Amazon Delivery*. 2018. Disponível em: <https://www.driving.co.uk/video/tesla-owner-wasnt-home-receive-amazon-delivery-solution-genius/>. Acesso em: 15 nov. 2018. Citado na página 34.

29 THE LINUX FOUNDATION. *Automotive Grade Linux*. 2018. Disponível em: <https://www.automotivelinux.org>. Acesso em: 15 nov. 2018. Citado na página 35.

30 INFOSEC INSTITUTE. *Qualitative Risk Analysis with the DREAD Model*. 2014. Disponível em: <https://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model>. Acesso em: 15 nov. 2018. Citado na página 41.

31 THE SOFTWARE ENGINEERING INSTITUTE. *The CERT Division*. 2018. Disponível em: <https://www.cert.org>. Acesso em: 15 nov. 2018. Citado na página 43.

32 SEACORD, R. C. *Secure Coding in C and C++*. 2. ed. Indianapolis: Addison-Wesley Professional, 2013. Citado na página 43.

33 KAMKAR, S. *Drive It Like You Hacked It*. 2015. Disponível em: <http://samy.pl/defcon2015/2015-defcon.pdf>. Acesso em: 15 nov. 2018. Citado na página 44.

34 AUTO ESPORTE. *Carros com sistema keyless são presas fáceis para ladrões, diz estudo*. 2016. Disponível em: <http://g1.globo.com/carros/noticia/2016/03/carros-com-sistema-keyless-sao-presas-faceis-para-ladroes-diz-estudo.html>. Acesso em: 15 nov. 2018. Citado na página 44.

35 EXPRESS. *These cars can be hacked in seconds - Do you own one of them?* 2017. Disponível em: <https://www.express.co.uk/life-style/cars/806889/Keyless-entry-car-keys-hack-theft-warning>. Acesso em: 15 nov. 2018. Citado na página 44.

36 SCHNEIER, B. *Man-in-the-Middle Attack against Electronic Car-Door Openers*. 2017. Disponível em: <https://www.schneier.com/blog/archives/2017/11/man-in-the-midd_8.html>. Acesso em: 15 nov. 2018. Citado na página 44.

37 SCHNEIER, B. *USB Kill Stick*. 2016. Disponível em: <https://www.schneier.com/blog/archives/2016/09/usb_kill_stick.html>. Acesso em: 15 nov. 2018. Citado na página 44.

38 USB KILL. *USB Killer v3*. 2017. Disponível em: <https://www.usbkill.com/products/usb-killer-v3>. Acesso em: 15 nov. 2018. Citado na página 44.

39 BONO, S. C. et al. *Security Analysis of a Cryptographically-Enabled RFID Device*. 2005. Disponível em: <https://www.usenix.org/legacy/events/sec05/tech/bono/bono.pdf>. Acesso em: 15 nov. 2018. Citado na página 45.

40 SCHIELI, N. *Open Immobilizer System: How Open-source Peer Reviewing Shifts the Security Paradigm*. 2011. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/article_open_immob_system.pdf>. Acesso em: 15 nov. 2018. Citado na página 46.

41 TILLICH, S.; WÓJCIK, M. *Security Analysis of an Open Car Immobilizer Protocol Stack*. 2012. Disponível em: <https://eprint.iacr.org/2012/617.pdf>. Acesso em: 15 nov. 2018. Citado na página 46.

42 MAGGI, F. *A Vulnerability in Modern Automotive Standards and How We Exploited It*. 2017. Disponível em: <https://documents.trendmicro.com/assets/A-Vulnerability-in-Modern-Automotive-Standards-and-How-We-Exploited-It.pdf>. Acesso em: 15 nov. 2018. Citado 2 vezes nas páginas 46 e 47.