VULNERABILIDADE EM SISTEMAS AUTOMOTIVOS

Marcelo Pires de Souza[1], Ricardo de Andrade[2] e Jorge Tomioka[1]

[1]UFABC – Universidade Federal do ABC
[2]Escola Politécnica - USP Universidade de São Paulo

E-mails: marcelo.s@ufabc.edu.br, ricardo-andrade@usp.br, jorge.tomioka@ufabc.edu.br

RESUMO

Os veículos modernos são constituídos por uma complexa rede interna informatizada e pode ser vulnerável a ataques maliciosos. Este trabalho tem como objetivo, colocar em pauta as possíveis fragilidades de seguranças a ataques encontradas atualmente nos chamados "carros inteligentes". Mesmo com relatos de insegurança nos sistemas embarcados dos veículos já apresentados em estudos anteriores e alguns ataques já catalogados, esse tema ainda é pouco discutido no Brasil e na maioria das vezes visto como irreal. Estudos evidenciam que há uma grande probabilidade de exploração remota através de conexões como: *Bluetooth*, USB (*Universal Serial Bus*), leitores de CD (*Compact Disc*), celular, Internet, entre outras, e ainda que tais conexões permitam o acesso sem fio possibilitando que intrusos façam o controle de diversos componentes do veículo (freios, motores, luzes, buzinas, entre outros) a longas distâncias, bem como a adulteração de dados. Relatos de ingerências locais através do conector OBD II (*On Board Diagnostics II*) também são comuns, adulteração de odômetro é habitualmente praticada no segmento de veículos seminovos. Este trabalho dá destaque a um ponto pouco explorado e traz para discussão um problema a ser mitigado pelo setor automotivo que a cada dia fica mais aderente a nova tendência de tecnologia, a "internet das coisas".

Palavras-Chave: Carros Inteligentes, Eletrônica Embarcada, Sistemas Automotivos, Ataques Maliciosos, OBD II, Internet das Coisas.

INTRODUÇÃO

O início desta década atingiu a marca de 1 bilhão de veículos automotores terrestre (carros, motocicletas, ônibus, caminhões e assemelhados), produzido em nosso planeta [1]. Nos últimos 20 anos têm sido incrementados a tecnologia dos carros sistemas eletromecânicos, principalmente com a introdução crescente de dispositivos da eletrônica em geral. Isso tem se viabilizado graças ao custo decrescente dos componentes eletrônicos, principalmente no que tange aos sensores, atuadores e micro controladores com integração cada vez maior, aliado com o alto grau de confiabilidade.

Comunicação entre veículos e a infraestrutura viária são temas altamente explorados nos últimos tempos com o intuito de se melhorar a segurança veicular, segurança no trânsito e a mobilidade pessoal. Com a implantação dessas inovações nos veículos as estradas se tornarão mais seguras, haverá diminuições nos congestionamentos, as atuais *tags* de pedágio, que atualmente apenas identificam os veículos, passarão com o advento das redes de comunicação

entre veículos a transmitir informações sobre vias, valores pagos e próximos pedágios, além de avisos de acidentes, condições de trânsito e obras.

A comunicação entre veículos (*car-to-car*) ou (*car-to-X*) infraestrutura, pode colaborar para que os sinais tráfego sejam ajustados de acordo com a quantidade de carros em um determinado trecho, além disso, viaturas de polícia, bombeiros ou ambulâncias podem contribuir com ainda mais dados, já que são automóveis com altos índices de circulação nas cidades.

As tecnologias relacionadas a esse segmento incluem ainda:

Frenagens de emergência: nas vias, durante o deslocamento dos veículos, mensagens podem ser transmitidas em situações em que o condutor submeter o veículo a uma frenagem de emergência, o grande diferencial é que não necessariamente os veículos devem estar no alcance de visão dos motoristas, mitigando assim diversos acidentes.

Tráfego *on-line*: informações de trânsito são compartilhadas durante todo o trajeto do veículo, identificando situações de congestionamentos, acidentes e tráfego intenso.

Inconsistências de vias: troca de informações de reparações e obstruções de vias e impedimentos de tráfego fora da normalidade entre os veículos.

Conexões com internet: possibilita a implementação de diversos serviços oferecidos atualmente pelas montadoras de veículos, *On Call* (Volvo), *OnStar* (Chevrolet), *App Connect* (Volkswagen), *Alexa* (Ford), entre outros.

Nos dias atuais, a evolução das tecnologias automotivas está cada vez mais dedicada a itens de conforto, conveniência e segurança, tais como: dirigibilidade, durabilidade, conectividade, multimídia, frenagem e eficiência energética.

Atualmente no desenvolvimento de um veículo 30% dos custos são empregados aos sistemas eletrônicos e 90% das inovações tecnológicas estão ligadas a sistemas eletrônicos, fazendo com que os veículos modernos cheguem a compreender até 80 unidades de controle eletrônico (ECU - *Electronic Control Unit*)[1] e uma complexa rede interna informatizada, constituída por sistemas que compreendem milhões de linhas de códigos, executado em dezenas de processadores heterogêneos com uma ligação abundante fornecida por redes internas (ex. CAN - *Controller Area Network*) [3].

No entanto com o incremento dessas mudanças, os veículos modernos correm riscos e se tornaram alvos fáceis, vulneráveis a ataques maliciosos. Trabalhos anteriores já demonstraram que um intruso conectado à rede interna de um carro pode burlar todos os sistemas de controle do computador, incluindo a segurança elementos críticos, como os freios e motores [3].

[1]As unidades de controle eletrônico – ECU, desenvolvidas para o uso veicular possuem projetos semelhantes. Sua estrutura pode ser subdivida no condicionamento do sinal de entrada, no processamento lógico desses sinais, no microcomputador e na saída dos níveis lógicos e de potência, como sinal de regulação ou comando [3].

Tais vulnerabilidades tem gerado uma grande abertura aos sistemas embarcados automotivos e algumas fragilidades já são observadas com certa frequência. Adulteração de odômetro é algo comumente praticado no segmento de veículos usados, como forma de aumentar o valor da revenda.

O objetivo deste estudo é identificar as falhas de segurança e privacidade, utilizadas nos veículos atuais, também chamados de “carros inteligentes”. Estudos apontam que intrusos que podem assumir o controle de um veículo ou daqueles que desejam reunir e utilizar dados pessoais do condutor.

Os intrusos podem acessar o veículo por intermédio de conexões sem fio *Bluetooth*, de conexões físicas OBD II[2], de um vírus em um "*smartphone*" conectado ao veículo ou até mesmo de um CD infectado lido por um sistema de áudio do veículo.

1. INFORMAÇÕES GERAIS

Os principais protocolos de comunicação empregados nos sistemas automotivos existentes são CAN, LIN, FlexRay e MOST [4].

Os sistemas automotivos em geral, são gerenciados a partir da ECU, o qual é composto de unidades do tipo sensores, atuadores e central de processamento.

Inicialmente, o processamento de controle era concebido na forma de uma arquitetura centralizada, de acordo com as limitações tecnológicas que existiam. Com a evolução dos microprocessadores e das redes de comunicação, a filosofia de processamento distribuído foi se destacando, principalmente pelas seguintes características:

- Redução de volume e quantidade de cabos;

- Redução de conectores;

[2]Em 1994, foi implantado o segundo estágio da legislação de diagnóstico na Califórnia, com o OBD II. Além das estipulações contidas no OBD I, agora a funcionalidade do sistema é monitorada (ex. os sinais do sensor são testados quanto à plausibilidade). O OBD II exige que todos os sistemas e componentes do gás de escapamento sejam monitorados, caso uma falha em um destes sistemas ou componentes provoque um aumento significativo nas emissões de gás de escapamento nocivo (limites de emissão OBD). Além disso todos os componentes usados para monitorar os componentes relacionados à emissão ou que afetam o resultado do diagnóstico, devem ser monitorados. As funções de diagnóstico para todos os componentes e sistemas inspecionados devem ser realizadas, normalmente, pelo menos uma vez no ciclo de teste do gás de escapamento. As funções de diagnóstico também devem operara um número suficiente de vezes, durante a operação normal do veículo no dia-a-dia. A partir do modelo de 2005, uma frequência específica de monitoramento (índice de desempenho de monitoração em uso) é necessária para muitas funções de monitoramento, durante a operação normal do veículo no dia-a-dia. A legislação foi revista várias vezes desde que o OBD II foi introduzido. A última atualização entrou em vigor a partir do modelo de 2004 [2].

- Redução de peso;

- Aumento de processamento;

- Facilidade de integração de novos sistemas;

- Facilidade de atualização, configuração e manutenção;

- Diagnósticos [5].

1.1. Controller Area Network – CAN

O protocolo CAN – *Controller Area Network*, desenvolvido inicialmente pela Bosch em 1986 é muito utilizado em aplicações de sistemas automotivos, reúne como características principais robustez e desempenho [6]. Conforme Veronesi (2005, p. 58 e 59), "o protocolo CAN é baseado na técnica de CSMA/CR (*Carrier Sense Multiple Access/Collision Resolution*), às vezes também chamado de CSMA/CD + AMP (*Carrier Sense Multiple Access/Collision Detection and Arbitration on Message Priority*), de acesso ao meio de transmissão. Isto significa que sempre que ocorrer uma colisão entre duas ou mais mensagens, a de mais alta prioridade terá o acesso ao meio físico assegurado e prosseguirá a transmissão" [7].

Como atributos básicos o barramento CAN possui as seguintes características: 8 bytes de dados, velocidade de até 1Mbit/s, priorização de mensagens, recepção *multicast* com sincronização, detecção de erros e sinalização e retransmissão automática de mensagens corrompidas [7]. Este conjunto de especificações assegura ao CAN simplicidade, alta confiabilidade, segurança e baixo custo [7]. Originalmente o protocolo CAN em sua primeira versão (CAN 2.0A), distinguia somente mensagens do tipo padrão, com identificadores de 11 bits, já o (CAN 2.0B), segunda versão deste protocolo, admite também mensagens estendidas com identificadores de 29 bits [7].

Em meados dos anos 2000, a produção dos microcontroladores CAN atingiu a marca de milhões ao ano, fabricação alavancada pela grande utilização deste protocolo nas indústrias do segmento automotivo. Fabricados pelas principais indústrias deste seguimento, destacam-se na produção de microcontroladores com controladores CAN integrados as empresas: Intel, Motorola, Philips, Siemens e Texas Instruments. Estes controladores podem ser encontrados na sua forma mais tradicional (circuito integrado), ou na forma de microcontroladores de 8, 16 e 32 bits com controladores CAN integrados [7].

Esse crescimento do CAN está fortemente ligado nas associações que foram feitas como a Cia (*CAN in Automation*) e a padronização do protocolo assim como o surgimento de várias empresas com soluções de diagnósticos, desenvolvimento de *softwares* e aplicação à rede CAN [8].

O grande interesse pelo barramento CAN foi devido às suas características que podem ser resumidas por:

- É baseado no conceito de broadcast [5].

- Um esquema de arbitragem não destrutiva (*bitwise arbitration*) descentralizada, baseada na adoção dos níveis dominante e recessivo, é usado para controlar o acesso ao barramento [7].

- As mensagens de dados são pequenas (no máximo oito *bytes* de dados) e são conferidas por *checksum* [5].

- Não há endereço explícito nas mensagens. Em vez disso, cada mensagem carrega um identificador que controla sua prioridade no barramento e que pode servir como uma identificação do conteúdo da mesma [7].

- Utiliza um elaborado esquema de tratamento de erros que resulta na retransmissão das mensagens que não são apropriadamente recebidas [5].

- Fornece meios efetivos para isolar falhas e remover nós com problemas do barramento [5].

- Oferece meios para filtragem das mensagens [7].

- O meio físico de transmissão pode ser escolhido de acordo com as necessidades. O mais comum é o par trançado, mas também podem ser utilizados outros meios de transmissão tais como fibra ótica e rádio frequência [5].

- Protocolo *standard* ISO [5];

- Capacidade de detectar e sinalizar erros [5];

- Capacidade multi-mestre [5];

- Capacidade *multicast* [5];

- Flexibilidade de configuração [5];

- Retransmissão automática de mensagens ”em espera” logo que o barramento esteja livre [5];

- Atribuição de prioridade às mensagens [5];

- Distinção entre erros temporários e erros permanentes dos nós [5];

- Elevadas taxas de transferência (1 Mbit/s) [5];

- Redução do cabeamento a ser utilizado [5];

- Baixo custo [5];

O *Controller Area Network* possui a propriedade de *broadcast*, ou seja, manda todos os dados na rede de forma síncrona (*bit* a *bit*). Além disso, possui um sistema de *bitwise arbitration* o qual possui um procedimento para ocorrências quando há colisões entre as mensagens no barramento. Ele gerencia as mensagens de acordo com a prioridade de recebimento. Por definição, o menor ID tem prioridade sobre os outros e consegue "ganhar' o barramento. Esse método é realizado através de *bits* dominantes (0) e *bits* recessivos (1). O *bit* dominante sobrescreve o *bit* recessivo até ter a prioridade no envio da mensagem [4].

A transmissão de dados possui uma relação com o comprimento de cabos. Quanto maior for o comprimento, menor será a taxa de transmissão.

1.2. Local Interconnect Network – LIN

O protocolo LIN – *Local Interconnect Network* é considerado por seus criadores como um *sub-bus* de CAN, LIN é usado principalmente em sistemas que não demandam alta velocidade (máximo de 20 kbit/s).

O principal desenvolvedor do conceito LIN foi a empresa Motorola (agora Freescale) e a primeira especificação, 'LIN rev. 0 ', surgiu em julho de 1999. Um consórcio logo foi criado, em março de 2000, incluindo diversos fabricantes como: Audi, BMW, Daimler Chrysler, Volkswagen e Volvo entre outras.

O protocolo LIN é destinado principalmente para apoiar o controle de elementos "mecatrônicos" encontrados em sistemas e aplicações veiculares.

O conceito do protocolo LIN consiste em um sistema de comunicação multiplexado, cujos níveis de performances então abaixo do CAN. Baseia-se no conceito de uma rede (sub), contendo apenas um mestre com um conjunto finito de nós escravos.

Como a rede é controlada pelo mestre, o sistema de comunicação é determinista, sendo totalmente dependente de um tempo sequenciamento fixado pelo controlador das tarefas.

O objetivo principal e original do LIN é proporcionar um 'sub-barramento' para o CAN, com funcionalidade reduzida e custos mais baixos, em outras palavras, para fornecer uma solução econômica, quando os níveis de desempenhos e requisitos não são elevados. Assim, ele pode ser utilizado em aplicações em que a taxa de bits e a largura de banda da rede são baixas e a alta confiabilidade e robustez não são exigidas como em aplicações como:

- Assentos (todos os ajustes do banco e funções);

- Portas (controles de vidros, retrovisores, etc);

- Controle de limpadores de para-brisas;

- Controle interno de luz, etc.

1.3. FlexRay

O protocolo *FlexRay* foi aplicado primeiramente em veículos de série pela empresa alemã BMW. Em 2006, os veículos X5 passaram a utilizar a rede para gerenciamento do seu sistema *Adaptive Drive*. O propósito da aplicação foi de utilizar este sistema como piloto para verificação e melhoria dos semicondutores e sistemas operacionais compatíveis com o protocolo, teste das ferramentas de projeto e monitoração disponíveis e comportamento do sistema em testes de EMC (*Electromagnetic Compatibility*) [9].

O sistema *Adaptive Drive*, estabiliza os amortecedores dos veículos, neutralizando as forças que agem no chassi, além de configurar a suspensão do veículo de acordo com o pavimento, assegurando uma viagem muito mais confortável para os passageiros. Este sistema utiliza sensores que mantém o veículo em uma altura constante, independente da sua carga e evita o efeito de rolamento nas curvas, para isto deve prover uma resposta imediata às variações do terreno.

O *FlexRay* transmite os seus dados via fibra óptica ou cabos de cobre a uma taxa de até 10 Mbit/s. De acordo com as especificações do protocolo a distância máxima de transmissão é de 24 metros [10]. Este valor é bem próximo daquele especificado para o protocolo CAN em sua velocidade máxima, a de 1Mbit/s.

O *FlexRay* conta com dois canais de comunicação, denominados “Canal A” e “Canal B”, que podem ser utilizados para a transmissão de um mesmo dado, ou para dados diferentes, dobrando a taxa nominal de transmissão.

Esta característica serve para atender a dois propósitos: no caso da transmissão de dados diferentes em cada um dos canais, a taxa de transmissão máxima da rede é dobrada para 20 Mbit/s. Já no caso da utilização dos dois canais para a redundância do sinal, ou seja, para a transmissão dos mesmos dados, esta característica oferece a robustez necessária para a substituição dos sistemas mecânicos por eletrônicos. Ainda, pode-se optar pela transmissão dos dados utilizando um único canal [11].

1.4. Media Oriented Systems Transport – MOST

O protocolo MOST – *Media Oriented Systems*, é um protocolo de comunicação veicular largamente utilizado em sistemas multimídias. Empregado em sistemas automotivos desde o início dos anos 2000, mais precisamente em 2001, em um BMW Série 7, apresentado no salão de Frankfurt do mesmo ano. Este protocolo se diferencia dos demais já apresentados por sua capacidade de transmissão, podendo ser esta via cabo ou fibra ótica, tornando o protocolo ainda mais eficiente quando aplicado a sistemas de entretenimento veicular [12].

MOST é mantido pela MOST *Cooperation*, uma cooperação entre as principais montadoras, fornecedores de autopeças e sistemistas do segmento automotivo, descantando-se como *partners:* Audi, BMW, Daimler, HARMAN, Microchip Technology e os parceiros integradores de sistemas China FAW Group, General

Motors, Honda, Hyundai/Kia, Jaguar, Land Rover, Porche, Toyota, Volkswagen e Volvo [13].

As redes MOST podem suportar até sessenta e quatro dispositivos ou nós. Este sistema utiliza topologia tipo anel, porém com sistema "*Plug and Play*", que permite adicionar ou remover dispositivos com muita facilidade. Quando da inserção de um novo dispositivo o sistema o reconhece automaticamente, ganhando agilidade e facilidade para o usuário.

A fibra óptica na rede MOST é muito veloz entre dispositivos, ela tem um par de portas e são montadas em anel. Os transmissores são diodos emissores de luz (LED´s) de 650 nm, com potência de 0,1 a 0,75 mW, e são diretamente modulados abaixo de 10dB. Os receptores são baseados em PIN fotodiodos. Os sinais são convertidos para forma eletrônica em cada dispositivo, sendo transmitido em volta de todo o anel.

O Sinal de transmissão para todos os dispositivos é sincronizado pelo "*Master Clock*", que faz o controle da rede. A rede requer dados sincronizados para 25Mbit/s para aplicações de vídeo, e manuseia dados assíncronos a 14,4 Mbits/s. O controle dedicado de canais requer 700 kbits/s. Todos os sinais analógicos são convertidos para sinais digitais antes da transmissão.

Benefícios da rede MOST:

- Baixo volume de fios na construção, ajuda a reduzir custos e espaço;

- Suporta temperaturas até 260ºC de acordo com IEC 68-2-20 para condições de todos os componentes soldados;

- Contatos elétricos do tipo MTS (Sistema de Micro Terminal) que suportam até 8A.

2. MODELOS DE AMEAÇAS

Ataques maliciosos podem surgir de diversas maneiras, os veículos podem ser acessados por meios físicos ou sem fio. Nesta seção abordaremos de forma abrangente os principais modelos de ameaças a um veículo moderno.

2.1. Acesso Físico

Automóveis modernos fornecem várias interfaces físicas que direta ou indiretamente permitem acessar as redes internas do carro. Acessos são concedidos através de interfaces físicas intermediárias [3].

2.1.1. OBD II

A interface do automóvel mais significativa é a porta OBD II, que normalmente fornece acesso direto ao barramento CAN do automóvel, suficiente a comprometer toda a gama dos sistemas automotivos. Comumente acessado durante as manutenções de rotina por técnicos, mecânicos e prestadores de serviço, para efetuar diagnósticos e programações na ECU [3].

2.1.2. Entretenimento

Outra classe importante de interfaces físicas está focada em sistemas de entretenimento. Praticamente todos os automóveis modernos possuem sistemas capazes de suportar um CD player apto a interpretar uma ampla variedade de formatos de áudio (MP3, WMA, e assim por diante). Da mesma forma, os fabricantes de veículos também fornecer algum tipo de porta de multimídia digital externo (Normalmente uma porta USB ou uma ligação para outros dispositivos) para permitir aos usuários controlar a mídia do seu carro. Consequentemente, um "intruso" pode submeter através da entrada de CD algum tipo de codificação maliciosa. Sendo assim, contra intuitivamente, um leitor de CD comprometido pode oferecer um eficaz caminho de ataque para os demais componentes automotivos [3].

2.2. Acesso Sem Fio

Os veículos atuais são dotados de infraestrutura para comunicações sem fio, o que permite a transmissão de dados e informações sem a necessidade do uso de cabos. Conexões maliciosas podem ser estabelecidas através de um transmissor sem fio na proximidade do receptor do carro com alcance entre 5 e 300 metros (curto alcance), podendo chegar a distâncias superiores a 1 km, utilizando canais de acesso digitais (longo alcance).

2.2.1. Bluetooth

Esse tipo de conexão tornou-se padrão em veículos populares vendidos por todos os fabricantes de automóveis. Com um alcance em torno de 10 metros, pode ser estendido através de amplificadores e antenas direcionais [3].

2.2.2. RFID – Chave do Veículo

Imobilizadores de veículos baseados em RFID agora são quase universais em automóveis modernos e são obrigatórios em muitos países em todo o mundo. Estes sistemas de incorporar um *tag* RFID em um chaveiro ou chave e um leitor próximo a coluna de direção do carro. Estes sistemas podem evitar que o carro entre em operação a não ser que a chave correta (conforme verificado pela presença da correta *tag* RFID) esteja presente.

2.2.3. Canais de Transmissão

São canais que não são especificamente destinados para um dado automóvel, mas pode ser "sintonizado" pelos receptores sob demanda. Conexões de ataque externo, transmissão de longo alcance, pode ser atraente como canais de controle (ou seja, para o desencadeamento de ataques) uma vez que, são capazes de efetivar comandos aos receptores simultaneamente e não requerem informações precisas de endereçamento para seus alvos [3].

Os automóveis modernos possuem uma infinidade de canais de transmissão: Sistema de Posicionamento Global (GPS), rádios digitais, RDS (*Radio Data System)*, etc.

Tabela abaixo apresenta a vulnerabilidades aos ataques maliciosos, suas classes de fragilidades, principais canais de acesso e escala.

Classe de Vulnerabilidade	Canal	Capacidade de Implementação	Visível ao Usuário	Escala	Controle Total	Custo
Físico Direto	Porta OBD-II	Ataque direto através do hardware diretamente no carro, porta OBD-II	Sim	Pequeno	Sim	Baixo
Físico Indireto	CD/DVD/Micro SD	Atualização de firmware baseada em CD	Sim	Pequeno	Sim	Médio
	CD/DVD/Micro SD	Música em formato (WMA)	Sim	Médio	Sim	Médio ~ Alto
	Porta de Entrada	WiFi ou conexões com fio de dispositivos	Não	Grande	Sim	Baixo
Curto Alcance Sem Fio	Bluetooth	Emparelhamento com aparelhos celulares infectados	Não	Grande	Sim	Baixo ~ Médio
Longo Alcance Sem Fio	Celular	Conexões, utilizando laptop ou telefones	Não	Grande	Sim	Médio ~ Alto

Tabela 1: Vulnerabilidades a ataques. Adaptado de [3].

A primeira coluna “classe de vulnerabilidade” apresenta a condição em que se faz o acesso ao veículo, esse ingresso pode ser local (físico direto e indireto) ou através de uma rede sem fio de curto ou longo alcance. Já a segunda coluna “canal” apresenta os diversos meios de acesso ao veículo (porta OBD-II, Celular, CD, entre outros). Os itens referentes à “capacidade de implementação” expressam algumas modalidades de hospedagem dos arquivos ou acessos maliciosos, que em algumas ocasiões podem ser imperceptíveis aos usuários conforme apresentado na coluna quatro. A proporcionalidade das inferências pode ser avaliada na coluna “escala” e algo de bastante relevância é que em todas as condições dispostas o controle do automóvel é total conforme manifestado no pilar “controle total”. A última coluna faz referência aos custos de implementação do ataque, que podem variar de acordo com a complexidade do acesso.

3. PRINCIPAIS ATAQUES CATALOGADOS

Apresentaremos agora alguns dos possíveis cenários de ataques já catalogados em trabalhos anteriores, onde diversos componentes de maneira individuais foram alterados ou manipulados através de intervenções externas.

3.1. Odômetro e Velocímetro

Adulteração de odômetro é algo comumente praticado no segmento de veículos usados, como forma de aumentar o valor da revenda.

Velocímetros podem ser manipulados para exibir uma velocidade arbitrária (apresentar uma velocidade irreal, por exemplo, metade da velocidade real). Tal ataque poderia, por exemplo, enganar um motorista para condução muito rápido.

3.2. Luzes Indicativas

Intervenções maliciosas podem desativar algumas luzes internas e externas no carro. Pacotes podem ser enviados para desativar todas as luzes do carro quando se atingir uma determinada velocidade, o que é particularmente perigoso, quando se aplica em condução. Isso inclui os faróis, as luzes de freio, as luzes auxiliares, as luzes internas, a iluminação do conjunto do painel de instrumento e outras luzes visor, no interior o carro. Pode-se imaginar que este ataque seja extremamente perigoso em uma situação em que uma vítima está dirigindo em alta velocidade à noite, em um ambiente escuro. O motorista não teria uma visão frontal, nem os indicadores do painel de instrumentos, e pessoas em outros carros não seriam capaz de ver a vítima [14].

3.3. Componentes Diversos

Experimentos realizados apresentaram controle sobre vários componentes do automóvel o que poderia gerar um total desconforto e pânico entre os ocupantes do veículo. Acionamento da buzina, limpadores de para-brisas, bloqueio de portas (ou impedimento que os ocupantes façam o desbloqueio das portas), acionamentos de vidro elétricos, ou até mesmo o desligamento do motor e o acionamento dos freios são intervenções que podem ser realizadas com o incremento de algumas linhas de códigos maliciosos às ECU’s dos automóveis.

4. DISCUSSÕES

Com a grande variedade de redes veiculares vem se investigando possibilidade de se trabalhar com o desenvolvimento de arquiteturas globais (desenvolvimento de hardware, software e comunicação entre os módulos automotivos), o que auxiliaria de forma significativa na redução dos custos.

O principal motivo para a criação de um padrão para o desenvolvimento de módulos eletrônicos automotivos é reduzir a complexidade atualmente existente quando se trata de novas tecnologias e novos desenvolvimentos. Com a falta de um padrão, este desenvolvimento acaba sendo repetido de acordo com cada montadora e cada fornecedor automotivo.

Devido a inúmeras inovações se faz necessário gerenciar este crescimento de demanda de módulos eletrônicos e *software* automotivos. A principal característica esperada desta padronização é a criação de um reúso entre as plataformas de uma mesma montadora, e principalmente que estes *softwares* possam ser utilizados entre diversas montadoras, aumentando assim a confiabilidade e a qualidade do sistema.

As primeiras discussões sérias e análises da necessidade de se criar e desenvolver arquiteturas globais para o setor automotivo surgiram em 2003 com a criação da AUTOSAR (***AUT****omotive* ***O****pen* ***S****ystem* ***AR****chitecture*), que é uma cooperação mundial entre as montadoras, fornecedores e outras empresas do ramo de eletrônicos, semicondutores e *software*, que tem como objetivo trabalhar no desenvolvimento e introdução de um padrão aberto de arquitetura de *software* para as indústrias automotivas.

CONCLUSÃO

Com a evolução dos automóveis, começaram a ter a necessidade de controles eletrônicos além dos habituais controles mecânicos. Estes foram evoluindo, passando a ocupar uma parte substancial do controle de todo o veículo, este aumento exponencial de controles e sensores no automóvel, tornou-se necessário a criação de diversos protocolos de comunicação para que entre todos estes controles houvesse um menor número de ligações possível bem como para a estipulação de uma hierarquia na resposta às diferentes solicitações.

A grande versatilidade dos protocolos de comunicações e os complexos sistemas de transmissão de dados dos veículos modernos apresentam reais vulnerabilidades, o que significa uma grande ameaça para os automóveis e seus condutores que a cada dia estão mais conectados.

Automóveis infectados podem causar uma gama de perturbações e danos, e este é um grande desafio a ser enfrentado no que diz respeito à segurança dos novos sistemas de automação veicular que vem se mostrando em diversos estudos frágeis, uma vez que suas ECUs podem ser manipuladas.

REFERÊNCIAS

[1] SILVA, Rafael Luiz da. **Caracterização do sinal do fenômeno de detonação utilizando filtros adaptativos e estimador de potência**. Tese de Doutorado. Universidade de São Paulo. 2014.

[2] BOSH, Robert. **Manual de Tecnologia Automotiva.** São Paulo. 25ª Ed. Editora Edgard Blücher, ISBN 2005.

[3] CHECKOWAY, Stephen; McCOY, Damon; KANTOR, Brian; ANDERSON Danny; SHACHAM, Hovav; SAVAGE, Stefan; KOSCHER, Karl; CZESKIS, Alexei; ROESNER, Franziska, KOHNO, Tadayoshi. **Comprehensive Experimental Analyses of Automo**tive Attack Surfaces. USENIX Secutiry Symposium. 2011.

[4] NICOLAS, Navet; FRANÇOIS, Simonot-Lion. **In-vehicle Communication Networks – A historical perspective and review.** Chapitre d´ouvrage: ZURAWSKI, Richard. **Industrial Communication Technology Handbook,** Second Edition, CRC Press Taylor&Francis, ISBN 2013.

[5] SANTOS, Max Mauro Dias; STEMMER, Marcelo Ricardo. **Redes Industriais sob a tecnologia CAN: DeviceNet, CANOpen e SDR.** São Paulo. Copyright Instrument Society of America, ISBN 2005.

[6] SILVA, Derick Henrique de Jesus. **Implementação de uma rede CANOPEN para controle de veículos autônomos**. Monografia (Graduação em Engenharia de Controle e Automação) – Universidade Federal de Minas Gerais 2011.

[7] VERONESI, Ricardo Luís Martins. **RTRASSOC51 – Módulo de Comunicação I2C Reconfigurável. rI2C**. Monografia (Mestrado em Ciência da Computação) – Centro Universitário Eurípides de Marília. 2005.

[8] Sato, Thiago Kenji Batisti. **Sistema Automotivo e Notificação de Acidente**. Monografia (Graduação em Engenharia Elétrica) – Universidade Federal do Paraná. Curitiba. 2010.

[9] SCHEDL, Anton. **Goals and Architecture of FlexRay at BMW**. Vector FlexRay Symposium, Stuttgart, 2007.

[10] FLEXRAY CONSORTIUM. **FlexRay Communications System Protocol Specification Version 2.1.** 245 f. 2005, The FlexRay Consortium.

[11] PARET, Dominique. **Multiplexed Networks for Embedded Systems.** Inglaterra: John Wiley & Sons, ISBN 2007.

[12] Frohlich, Antônio Augusto; Souza, Diego Tondo e Bratti, Diogo. **Sistemas Automotivos Embarcados**. UFSC – INE5355 – Sistemas Operacionais. Novembro. 2008.

[13] MOST Cooperation. **MOST Specification Rev. 2.4 - 05/2005.** Germany, 1999.

[14] KOSCHER, Karl; CZESKIS, Alexei; ROESNER, Franziska, PATEL, Shwetak; KOHNO, Tadayoshi; CHECKOWAY, Stephen; McCOY, Damon; KANTOR, Brian; ANDERSON Danny; SHACHAM, Hovav; SAVAGE, Stefan. **Experimental Security Analysis of Modern Automobile.** IEEE Symposium on Security and Privacy, Oakland, CA, May, 2010.