VI Simpósio de Iniciação Científica 2023
Ciência como ferramenta de transformação da sociedade

LEVANTAMENTO DE VULNERABILIDADES NOS SISTEMAS ELETRO-ELETRÔNICOS AUTOMOTIVOS

Leonardo Sousa Ferreira Fadul[1] (IC), Otávio de S. M. Gomes (PQ)[1]
[1]*Universidade Federal de Itajubá*

Palavras-chave: Criptografia. Protocolos. Scanner. Sistemas Automotivos. Vulnerabilidades.

Introdução

A evolução da tecnologia automotiva é longa e diversificada que abrange mais de um século de inovações contínuas, transformando carros de simples veículos motorizados em sofisticadas máquinas de alta tecnologia. Ao longo dos anos, inúmeros componentes e tecnologias foram introduzidos, redefinindo a forma como vivemos, trabalhamos e nos deslocamos.

A crescente integração de tecnologia em veículos automotivos modernos trouxe consigo uma série de benefícios, como maior segurança, eficiência e comodidade. No entanto, essa conectividade também introduziu um novo conjunto de desafios, particularmente no que diz respeito à cibersegurança. A presente pesquisa tem como objetivo explorar a área da cibersegurança e análise de vulnerabilidades em sistemas automotivos inteligentes, investigando as ameaças em potencial que podem afetar a segurança e privacidade dos ocupantes e a integridade dos veículos.

À medida que os veículos se tornam cada vez mais conectados e autônomos, a exposição a riscos cibernéticos cresce significativamente. Ataques de hackers podem não apenas comprometer a segurança dos passageiros, mas também interromper o funcionamento de sistemas críticos de um veículo, resultando em graves acidentes. O objetivo da pesquisa é, portanto, realizar um levantamento inicial destas ameaças.

Metodologia

Durante o desenvolvimento desta pesquisa sobre cibersegurança e análise de vulnerabilidades em sistemas automotivos inteligentes, a abordagem adotada consistiu em um levantamento do estado da arte de soluções nesta área.

Primeiramente, conduziu-se uma revisão da literatura e análise do estado da arte, focando nas vulnerabilidades relacionadas à comunicação em sistemas embarcados e na cibersegurança, com ênfase na arquitetura AUTOSAR. Também foi feito um estudo sobre os principais protocolos de comunicação automotiva, como o CAN, LIN, FlexRay, MOST e Ethernet.

Em seguida, realizou-se um estudo sobre algoritmos de criptografia e técnicas de segurança empregados no contexto da IoT para proteção de dados em dispositivos embarcados, com uma aplicação específica nas vulnerabilidades de sistemas automotivos inteligentes.

Posteriormente, efetuou-se uma análise das vulnerabilidades mais notórias em sistemas automotivos, abordando aspectos como o sequestro de unidades de controle eletrônico (ECU), comprometimento via smartphone emparelhado, vulnerabilidades de comunicação veículo-para-tudo (V2X) e veículo-para-veículo (V2V), exposição excessiva de dados pessoais, questões relacionadas a proprietários/locatários anteriores e a confiança na conectividade de rede.

Resultados e discussão

Desde os primórdios dos veículos motorizados até os carros altamente sofisticados e autônomos de hoje, a indústria automotiva tem constantemente se reinventado para atender às demandas crescentes por eficiência, segurança, conforto e sustentabilidade. A adoção de motores a combustão interna (década de 1870) **[1]** e a melhoria da eficiência dos motores contribuíram para aumentar a velocidade e o alcance dos veículos. Inovações como a introdução de sistemas de

frenagem assistida(1978) **[2]**, direção hidráulica(1920) **[3]**, transmissões automáticas(1930) **[4]** e sistemas de segurança passiva, como cintos de segurança(1903) **[5]** e airbags(1974) **[6]**. A década de 1980 testemunhou o uso crescente de eletrônica nos carros, com a incorporação de sistemas de injeção eletrônica de combustível(1957) **[7]** e computadores de bordo(1970) **[8]**.

Os protocolos de comunicação automotiva desempenham papéis cruciais na interconexão de dispositivos em veículos modernos, facilitando a comunicação entre as Unidades de Controle Eletrônico (ECUs) de maneira eficiente e confiável. O protocolo CAN, com seus diferenciais de tensão, proporciona uma comunicação robusta e é amplamente adotado na indústria automotiva **[9]**.

O LIN, por sua vez, oferece uma alternativa econômica para dispositivos de baixa prioridade, utilizando um único cabo bidirecional e taxas de transferência de dados mais baixas **[10]**. O FlexRay se destaca por sua alta taxa de transferência e flexibilidade, sendo adequado para aplicações que requerem determinismo e previsibilidade no fluxo de dados, como sistemas de controle avançados e segurança ativa **[11]**.

Já o MOST utiliza fibra óptica para garantir alta velocidade e imunidade a interferências, com uma arquitetura que permite sincronização precisa entre os dispositivos, resultando em uma comunicação coordenada e confiável **[12]**. Cada um desses protocolos desempenha um papel fundamental na criação de sistemas automotivos avançados e eficazes.

Apesar dos avanços em proteção e segurança, os sistemas automotivos continuam sendo alvos de ataques cibernéticos, especialmente à medida que os veículos se tornam mais conectados e dependentes de tecnologia digital **[13]**.

A criptografia desempenha um papel fundamental na mitigação desses riscos, garantindo a integridade dos sistemas e a segurança dos ocupantes. Ela envolve a codificação de dados em um formato que só pode ser lido após ser decifrado, sendo essencial para proteger a privacidade e a segurança das informações. Existem dois principais tipos de criptografia: a simétrica, que utiliza uma única chave compartilhada para cifrar e decifrar dados, e a assimétrica, que emprega duas chaves relacionadas, uma pública e outra privada, para fins de cifragem e decifragem, garantindo a segurança dos dados mesmo com a divulgação da chave pública.

O Advanced Encryption Standard (AES) é um algoritmo de criptografia de blocos desenvolvido pelo NIST em 2001. Ele opera em blocos de 128 bits, usando chaves privadas de 128, 192 ou 256 bits para determinar o número de rodadas (10, 12 ou 14) no processo de cifragem e decifragem **[14]**.

O algoritmo Blowfish, desenvolvido por Bruce Schneier em 1993, é de domínio público, sem patentes ou licenças. É uma criptografia de bloco simétrico, com blocos de 64 bits. A chave privada varia de 32 a 448 bits, gerando 18 subchaves em 16 rodadas **[15]**.

O algoritmo Camellia, criado em 2000 pela Nippon Telegraph e Mitsubishi Electric Corporation, é patenteado, mas está disponível para uso sem royalties. É um algoritmo de criptografia de bloco simétrico que opera em blocos de 128 bits com chaves privadas de 128, 192 ou 256 bits **[16]**.

O algoritmo CAST, criado por Carlisle Adams e Stafford Tavares em 1996, é patenteado, mas oferece licença sem royalties. Trata-se de um algoritmo de criptografia de bloco simétrico que opera em blocos de 64 bits, com chaves privadas de 128 ou 256 bits **[17]**.

A vulnerabilidade das portas de diagnóstico OBD-II é uma crescente preocupação na segurança de veículos automotivos **[18]**. Essas portas, presentes na maioria dos veículos fabricados desde a década de 1990, facilitam a conexão de equipamentos de diagnóstico ao sistema do veículo, permitindo análise rápida de problemas. No entanto, a interface OBD-II proporciona acesso completo ao barramento CAN, possibilitando intervenções no tráfego do veículo e potenciais alterações em funções críticas de segurança, uma vez que ambas as interfaces não oferecem proteção por padrão **[19]**.

Preocupações relacionadas à vulnerabilidade da porta OBD-II incluem acesso não autorizado, onde invasores podem conectar dispositivos para acessar sistemas críticos do veículo, e manipulação da ECU, que permite aos invasores modificar o firmware da ECU para controlar o desempenho do veículo ou desativar sistemas de segurança.

Já os ataques de rede visam explorar vulnerabilidades nos sistemas de comunicação de uma rede, com o objetivo de interromper o funcionamento,

roubar informações ou comprometer a integridade dos sistemas conectados. As principais vulnerabilidades incluem os ataques de Negação de Serviço (DoS) **[20]**, que sobrecarregam recursos de um sistema, tornando-o inacessível. Nesse ataque, os invasores buscam sobrecarregar a rede CAN com mensagens de alta prioridade, impedindo que outras mensagens com menor prioridade sejam lidas, o que acaba prejudicando sistemas críticos como frenagem e direção assistida. Outro tipo de ataque conhecido é o ataque Man-in-the-Middle (MitM) **[21]**, onde um invasor intercepta e modifica comunicações entre veículos legítimos, expondo informações sensíveis e propagando informações incorretas pela rede.

Os ataques de spoofing envolvem falsificar informações para enganar sistemas automotivos, como no caso do spoofing de GPS **[22]**, em que um atacante cria sinais falsos para fornecer informações de localização incorretas aos veículos. Isso pode levar a situações perigosas, como desvio de rotas e colisões. Essas vulnerabilidades ocorrem devido à previsibilidade das características dos sinais de GPS, permitindo que invasores criem sinais falsos semelhantes para enganar os sistemas.

Há também a vulnerabilidade de smartphones emparelhados via Bluetooth com sistemas automotivos **[23]**, uma preocupação em termos de segurança cibernética nos veículos modernos. Quando um smartphone é conectado ao sistema de entretenimento de um veículo, ele pode servir como uma porta de entrada para ataques cibernéticos, pois malwares em smartphones podem acessar o barramento CAN por meio da conexão Bluetooth.

Outro ponto importante é a garantia de que as informações coletadas pelos veículos permaneçam seguras e confidenciais é essencial para construir a confiança dos usuários nesses sistemas. Os fabricantes de automóveis podem adotar soluções de cibersegurança para proteger dados pessoais e informações corporativas sensíveis. Isso inclui a implementação de medidas de segurança básicas, como firewalls e antimalware, para prevenir ataques de ransomware e malware **[24]**.

A partir deste levantamento, viu-se a oportunidade de desenvolvimento de um scanner para o barramento CAN, que pode ser implementado para objetivos de testes de vulnerabilidades em sistemas automotivos. Essa ferramenta desempenharia um papel importante na segurança do veículo, pois permitiria que os engenheiros e pesquisadores identificassem possíveis pontos fracos no protocolo. Ao realizar varreduras minuciosas do barramento CAN, o scanner poderia detectar anomalias, intrusões ou tentativas de ataques, possibilitando a implementação de medidas proativas de segurança e a diminuição de riscos potenciais.

Conclusões

Este dispositivo desempenhará um papel importante na garantia da segurança cibernética de veículos, ajudando a identificar vulnerabilidades e potenciais pontos fracos em sistemas críticos. A contínua pesquisa nessa área é essencial, uma vez que as ameaças cibernéticas estão em constante evolução e se tornam cada vez mais sofisticadas. Investir em tecnologias avançadas de segurança, como scanners para o barramento CAN, não apenas protege vidas e recursos, mas também contribui para a confiabilidade dos sistemas em um mundo cada vez mais conectado.

Portanto, incentivar o desenvolvimento contínuo dessas ferramentas e a pesquisa em segurança cibernética é imperativo para enfrentar os desafios emergentes e garantir um futuro seguro e resiliente para a indústria automotiva.

Como continuidade deste projeto, espera-se realizar o desenvolvimento de um protótipo de scanner automotivo que realize a detecção das principais vulnerabilidades documentadas e conhecidas.

Agradecimentos

Gostaria de agradecer pela oportunidade de pesquisa de iniciação científica à Universidade Federal de Itajubá, ao orientador Otávio Gomes pela orientação e conhecimento que me ajudaram em minhas pesquisas, e ao órgão CNPq pela bolsa de pesquisa (PVDI277-2022). Também gostaria de agradecer aos meus pais por todo apoio que recebo todos os dias.

Referências

[1] ABM Peças, 2022. Breve história sobre a invenção do motor de combustão interna. Disponível em: https://blog.abmpecas.com/breve-historia-sobre-a-invencao-do-motor-de-combustao-interna/. Acesso em: 27 out. 2022.

[2] Panaro, Raphael. Quatro Rodas, 2018. Freios ABS completam 40 anos de história salvando vidas. Disponível em: https://quatrorodas.abril.com.br/especial/freios-abs-completa

m-40-anos-de-historia-salvando-vidas. Acesso em: 15 out. 2023.
[3] Malheiros, Péricles. Estadão, 2020. Conheça a história da direção hidráulica. Disponível em: https://jornaldocarro.estadao.com.br/fanaticos/conheca-historia-da-direcao-hidraulica/. Acesso em: 20 out. 2022.
[4] Auto Show Collection. A incrível história do câmbio automático. Disponível em: https://www.autoshowcollection.com.br/2019/03/09/a-incrivel-historia-do-cambio-automatico/. Acesso em: 27 out. 2022.
[5] BlaBlaCar Blog. 5 curiosidades sobre o cinto de segurança que você não sabia. Disponível em: https://blog.blablacar.com.br/blablalife/viagens/dicas/5-curiosidades-sobre-o-cinto-de-seguranca-que-voce-nao-sabia. Acesso em: 05 nov. 2022.
[6] Drives.today. First Production Car with Driver and Passenger Airbags: 1974 Oldsmobile Toronado. Disponível em: https://drives.today/articles/649/history/first-production-car-with-driver-and-passenger-airbags-1974-oldsmobile-toronado/votren-d.html. Acesso em: 05 nov. 2022.
[7] Reparação Automotiva. Conheça a história da injeção eletrônica. Disponível em: https://www.reparacaoautomotiva.com.br/2021/04/15/conheca-a-historia-da-injecao-eletronica/. Acesso em: 05 nov. 2022.
[8] OBD Experts. A brief history of OBD-II. Disponível em: https://www.obdexperts.co.uk/a-brief-history-of-obd-ii/. Acesso em: 15 jan. 2023.
[9] SORDI JUNIOR, Celio Heitor; SHIOHARA, Thomaz Weinrich. Sistema de comunicação e arquitetura baseado no protocolo CAN. 2013. 126 f. Trabalho de Conclusão de Curso (Graduação) – Universidade Tecnológica Federal do Paraná, Curitiba, 2013.
[10] AutoTechDrive. Autotechdrive. What Is LIN Protocol? - A Complete Guide. Disponível em: https://autotechdrive.com/what-is-lin-protocol-a-complete-guide/. Acesso em: 20 dez. 2022.
[11] NI. NI. NI, 2023. Disponível em: https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/flexray-automotive-communication-bus-overview.html. Acesso em: 22 dez. 2022.
[12] Andreas Grzemba. MOST THE AUTOMOTIVE MULTIMEDIA NETWORK FROM MOST25 TO MOST150. 2011.
[13] IEEE Innovation at Work. The Continuing Evolution of Automotive Cybersecurity. Disponível em: https://innovationatwork.ieee.org/the-continuing-evolution-of-automotive-cyber-security/. Acesso em: 19 jul. 2023.
[14] National Institute Of Standards and Technology. NIST. NIST.GOV, 2023. Disponível em: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development. Acesso em: 10 jan. 2023.
[15] Schneier, Bruce. The Blowfish Encryption Algorithm. Schneier. Disponível em: https://www.schneier.com/academic/blowfish/. Acesso em: 17 jan. 2023.
[16] Kazumaro AOKI, Tetsuya ICHIKAWA, etc., "Specification of Camellia -a 128-bit Block Cipher," Nippon Telegraphy and Telephone Corporation, Mitsubishi Electric Corporation, September 2001.
[17] Jadoon, Ahmer & Wang, Licheng & Li, Tong & Zia, Muhammad. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. Wireless Communications and Mobile Computing. 2018. 1-15. 10.1155/2018/1640167.
[18] Y. Takefuji, "Connected Vehicle Security Vulnerabilities [Commentary]," in *IEEE Technology and Society Magazine*, vol. 37, no. 1, pp. 15-18, March 2018, doi: 10.1109/MTS.2018.2795093.
[19] Ammar, Mahmoud & Janjua, Hassaan & Thangarajan, Ashok & Crispo, Bruno & Hughes, Danny. (2020). Securing the On-board Diagnostics Port (OBD-II) in Vehicles.
[20] Palanca, A.; Evenchick, E.; Maggi, F.; Zanero, S. A stealth, selective, link-layer denial-of-service attack against automotive networks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Bonn, Germany, 6–7 July 2017; Volume 10327, pp. 185–206.
[21] Adnane, Asma & Ahmad, Farhan & Franqueira, Virginia & Kurugollu, Fatih & liu, Lu. (2018). Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. Sensors. 18. 10.3390/s18114040.
[22] M. Kamal, A. Barua, C. Vitale, C. Laoudias and G. Ellinas, "GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles," 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021, pp. 1-7, doi: 10.1109/VTC2021-Fall52928.2021.9625567.
[23] C. Gao, G. Wang, W. Shi, Z. Wang and Y. Chen, "Autonomous Driving Security: State of the Art and Challenges," in IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7572-7595, 15 May 15, 2022, doi: 10.1109/JIOT.2021.3130054.
[24] Coos, Andrada. Endpoint Protector, 2021. Automotive Companies and Data Security. Disponível em: https://www.endpointprotector.com/blog/automotive-companies-and-data-security/. Acesso em: 05 abr. 2023.