UNIVERSIDADE ABERTA

UNIVERSIDADE
DE TRÁS-OS-MONTES
E ALTO DOURO

Verificação da validade de certificados criptográficos de unidades em veículos pela geração e distribuição de informação de *timestamp*

Felipe Fernandes

Mestrado em Engenharia Informática e Tecnologia Web

2024

UNIVERSIDADE ABERTA

Verificação da validade de certificados criptográficos de unidades em veículos pela geração e distribuição de informação de *timestamp*

Felipe Fernandes

Mestrado em Engenharia Informática e Tecnologia Web

Dissertação orientada pelo professor José Henrique P. São Mamede

Fevereiro 2024

Agradecimentos

A busca pelo conhecimento costuma vir acompanhada de muito esforço. Sempre foi assim na minha vida, desde os primeiros treinamentos técnicos, passando pela graduação e diversas especializações realizadas junto com a vida profissional continuada. O desafio para a conclusão desse trabalho não seria diferente. Um presente veio logo no início da jornada, minha filha Sarah, ainda em adaptação a um novo país junto com minha esposa Priscila e enfrentando uma pandemia no caminho. Nada disso seria possível se não fosse o apoio da minha família, principalmente da minha esposa.

Mudar para um novo país e começar um novo emprego torna-se muito mais fácil quando conhecemos pessoas que se tornam praticamente parte da sua família. Novamente, nada disso seria possível se não fosse a família de colegas da Jaguar Land Rover, que em cada etapa deste trabalho apoiou com informações, configuração das funcionalidades, suporte para a definição da solução e o desenvolvimento do artefato. Um agradecimento especial aos meus colegas Seil, Henrique, Saurabh, Walid, Shalom, Navdeep, Dilip e Samuel.

Desenvolver um trabalho de engenharia é muito desafiador, mas é diferente de fazer ciência. Aprender a fazer isso não seria possível sem o apoio e orientação do meu professor orientador José Henrique. A participação do retiro e todo o feedback recebido dos professores, em especial do professor Leonel Morgado, fizeram toda a diferença, por isso um grande obrigado a todos eles.

Por fim, agradeço a todos da UAB, profissionais e colegas de curso, que estiveram comigo juntos nessa jornada e contribuíram de diversas formas para o meu crescimento como profissional e pessoa.

Felipe Fernandes

Ennis, Irlanda, 2024

Dedicatória

Para minha filha Sarah, meu maior presente durante toda essa jornada...

DECLARAÇÃO DE INTEGRIDADE

STATEMENT OF INTEGRITY

Declaro ter atuado com integridade na elaboração da presente dissertação/tese. Confirmo que em todo o trabalho conducente à sua elaboração não recorri à prática de plágio ou a qualquer outra forma de falsificação de resultados. Mais declaro que tomei conhecimento integral do Regulamento Disciplinar da Universidade Aberta, publicado no Diário da República, 2.ª série, n.º 215, de 6 de novembro de 2013.

I hereby declare having conducted my thesis with integrity. I confirm that I have not used plagiarism or any form of falsification of results in the process of the thesis elaboration. I further declare that I have fully acknowledged Disciplinary Regulations of the Universidade Aberta (regulation published in the official journal Diário da República, 2.ª série, N.º 215, de 6 de novembro de 2013).

Universidade Aberta, 15 de fevereiro de 2024

Nome completo/Full name: Felipe Fernandes

Assinatura/Signature: 

Resumo

"Verificação da validade de certificados criptográficos de unidades em veículos pela geração e distribuição de informação de timestamp"

Não muito diferente de outras áreas que aderiram ao movimento de digitalização e conectividade que agora tem que lidar com o surgimento de ataques cibernéticos, a indústria automotiva que até algumas décadas atrás tinha que lidar apenas com segurança em termos de garantir o funcionamento correto do veículo no que se referre a qualidade, agora tem o tema da cibersegurança no centro das atenções. O desafio se torna ainda mais relevante à medida que governos preocupados com os impactos começam a legislar sobre o tema, exigindo que empresas que já estão sob pressão pela reinvenção digital o façam, levando o tema da segurança cibernética muito a sério. No entanto, diferentemente de outros ambientes da informática onde é possível analisar os riscos e depois implementar suas mitigações utilizando os melhores métodos e ferramentas disponíveis no mercado, a indústria automotiva tradicional tem suas arquiteturas eletrônicas baseadas no uso de dezenas de centrais eletrônicas, vindas de diferentes fornecedores e utilizando diferentes tecnologias, onde muitas vezes soluções customizadas são a única saída. A pesquisa deste trabalho tem como foco a identificação de uma solução para a validação de certificados de criptografia de forma segura, garantindo um tempo confiável de informações na central eletrônica no final da rede. Pesquisas durante a revisão literária demonstraram claramente a falta de uma solução pronta para o problema, o que resultou na proposição de uma solução dedicada ao problema dos automóveis. A implementação do artefato comprovou a eficácia da solução proposta contra os principais ataques, mas também demonstrou a limitação do uso da solução em termos de escalabilidade para o gerenciamento de um maior número de casos de uso, deixando uma porta aberta para a continuidade do trabalho.

Palavras-chave: Timestamp, Key Management, Automotive Electrical Architecture, Certificado, Criptografia, Design Research Science, Segurança da Informação, CAN, Ethernet, ECU, PKI, UNECE, UN155, Secure Time, Hash, HMAC, Automóveis, Montadoras, Servidor, Rede, Autenticação.

Abstract

"Verification of the validity of cryptographic certificates of units in vehicles by the generation and distribution of timestamp information"

Not unlike other areas joining the digitization and connectivity movement that now have to deal with the emergence of cyberattacks, the automotive industry that until a few decades ago had to deal only with safety, now has the theme of security at the center of attention. The challenge becomes even more relevant as governments concerned about the impacts begin to legislate on the subject, requiring companies that are already under pressure for digital reinvention to do so by taking the subject of cyber security very seriously. However, unlike other information technology environments where it is possible to analyze the risks and then implement their mitigations using the best methods and tools available in the market, the traditional automotive industry has its electronic architectures based on the use of dozens of electronic centrals, coming from different suppliers and using different technologies, where often customized solutions are the only way out. The research of this work focuses on the identification of a solution for the validation of encryption certificates in a secure way by ensuring a reliable time information in the electronic central at the end of the network. Research during the literature review clearly demonstrated the lack of an off-the-shelf solution to the problem, which resulted in the proposition of a solution dedicated to the problem of automobiles. The implementation of the artifact proved the effectiveness of the proposed solution against the main attacks, but also demonstrated the limitation of the use of the solution in terms of scalability for the management of a greater number of use cases, leaving an open door for the continuity of the work.

Keywords: Timestamp, Key Management, Automotive Electrical Architecture, Certificate, Cryptography, Design Research Science, Information Security, CAN, Ethernet, ECU, PKI, UNECE, UN155, Secure Time, Hash, HMAC, Automobiles, Automakers, Server, Network, Authentication.

Índice

Índice de Tabelas 9
Índice de Figuras 10
Lista de Definições & Siglas 11
Capítulo 1 Introdução 12
1.1 - Contexto 13
1.2 - Motivação 14
1.3 - Estrutura do Documento 15
Capítulo 2 Referencial Teórico 17
2.1 - Revisão da Literatura 18
2.2 - Discussão 53
Capítulo 3 Metodologia 55
3.1 - Como a Design Science Research foi utilizada nesse trabalho 58
Capítulo 4 Problemas e Objetivos 60
4.1 - Identificação e Conscientização do Problema 61
4.2 - Objetivos da Pesquisa 62
Capítulo 5 Proposta de Artefato 65
5.1 - Requisitos 66
5.2 - Proposição de um Modelo para Resolução do Problema 67
5.3 - Proposta 68
5.4 - Visão Geral 69
5.5 - Implementação 79
Capítulo 6 Demonstração, Avaliação e Conclusões 87
6.1 - Demonstração 88
6.2 - Avaliação 92
6.3 - Conclusões 94
Referências 99

Índice de Tabelas

Tabela 1 - Critérios de Seleção 21
Tabela 2 - Avaliação do Desenho do Estudo 22
Tabela 3 - Tamanho da Amostra e Avaliação da Seleção 22
Tabela 4 - Avaliação da Coleta e Análise de Dados 23
Tabela 5 - Avaliação da Validade e Confiabilidade 23
Tabela 6 - Avaliação da Considerações Éticas 23
Tabela 7 - Avaliação dos Relatórios e Documentação 24

Índice de Figuras

Figura 1 - Exemplo da aplicação da avaliação da qualidade do estudo 27
Figura 2 - Exemplo de extração de dados de estudos qualificados 28
Figura 3 - Exemplo de síntese de dados extraídos de estudos selecionados 29
Figura 4 - Design Science Research (Vaishnavi & Kuechler, 2004) 57
Figura 5 - Classes de problemas identificados. 63
Figura 6 - Formato de dados de Tempo 69
Figura 7 - Quadro de requisição de Tempo Seguro 70
Figura 8 - Quadro de resposta de Tempo Seguro 71
Figura 9 - Troca de chave de comunicação 73
Figura 10 - Quadro de resposta para o recebimento da chave de comunicação 73
Figura 11 - Processo de Trust Bonding e de distribuição da Com Key 73
Figura 12 - Solicitação e respota de Tempo Seguro com nonce 76
Figura 13 - Processo de distribuição de Tempo Seguro 78
Figura 14 - Escopo do artefato 80
Figura 15 - Estrutura de mensagens de solicitação de Tempo Seguro para artefato 80
Figura 16 - Estrutura de mensagem de resposta de Tempo Seguro para artefato 81
Figura 17 - Artefato proposto para avaliação do protocolo 82
Figura 18 - Placa de ECU end point (SECU) com conexões necessárias para se comunicar 83
Figura 19 - Raspberry Pi para acesso ao servidor usado conectar com a PECU 84
Figura 20 - Diagrama de implementação do artefato 84
Figura 21 - Vector VN5640: Switch que permite a comunicação entre os dispositivos 85
Figura 22 - Setup do artefato completo 86
Figura 23 - Rede monitorada com mensagens de solicitação e resposta de Tempo Seguro 88
Figure 24 - Rede monitorada com HMAC incorreto da SECU 90
Figura 25 - Rede monitorada com timestamp incorreto da SECU 91
Figura 26 - Rede monitorada com quadro HMAC incorreto 92

Lista de Definições & Siglas

Nome	Significado
ACK	Reconhecimento de um sinal ou mensagem recebida.
Ad-hoc	Expressão em latim que significa “para este fim” que no universo da tecnologia indica uma conexão temporária entre computadores para um propósito específico.
AutoSAR	Padrão de desenvolvimento de *software* para módulos eletrônicos automotivos
CAN	Controller Area Network é um padrão de rede automotiva amplamente utilizado para conectar as centrais eletrônicas.
CSMS	Sistema de Gestão de Segurança Cibernética exigido pela UN155 para a gestão de segurança cibernética dentro de uma montadora.
DoS	Negação de serviço, um tipo de ataque cibernético para interromper um serviço ou funcionalidade.
DSR	Metodologia Design Science Research.
ECU	Electronic Control Unit são pequenos computadores embarcados em veículos com funções específicas, como controlar o motor, e conectados formam o conceito de arquitetura eletrônica veicular.
EV	Categoria de veículos movidos a energia elétrica.
HMAC	Tipo de autenticação de mensagens usando funções de hash e chave criptográfica.
IPSec	Padrão de segurança para redes IP.
TI	Tecnologia da informação.
MACSec	Padrão de segurança ponto a ponto para links ethernet.
Nonce	Número arbitrário que só pode ser usado uma vez.
NTP	Network Time Protocol.
NTS	Network Time Security.
PECU	Primary ECU é a principal central do carro com maior capacidade de processamento, gerenciamento de segurança em *hardware* e conectividade.
PKI	Public Key Infrastructure.
PnC	Plug and Charge é a funcionalidade de pagar pelo carregamento de veículos elétricos a partir da própria conexão do cabo de carregamento usando o padrão ISO 15118.
PoC	Prova de conceito.
PTP	Precision Time Protocol
RTC	Real Time Clock é o *hardware* baseado em cristal para manutenção de tempo, clocking, dentro de um dispositivo eletrônico
SECU	Secondary ECU é a central na ponta da rede, geralmente com poucos recursos de processamento e memória para executar funções de segurança.
TB	Trust Bonding
UN155	Legislação da UNECE em vigor nos países membros, que visa garantir a correta gestão da segurança cibernética nas montadoras.
UNECE / UN	Comissão Económica para a Europa das Nações Unidas
UTC	Tempo Universal Coordenado
WP.29	Grupo UNECE responsável por escrever as normas e leis de segurança cibernética do grupo.
X.509	Padrão de certificado criptográfico

Capítulo 1
Introdução

1.1 - Contexto

Uma área-chave para permitir a escalada contínua de conectividade e funções autônomas em veículos modernos é a segurança cibernética. Como se não fossem apenas os casos de ataques ocorridos desde 2015 no mundo real contra grandes marcas como mostram Miller e Valasek (2015) [1] e as responsabilidades dessas marcas em proteger seus usuários e sua imagem, pela primeira vez uma série de legislações específicas estão sendo adotadas ao redor do mundo. Um primeiro grande passo foi dado pela UN155 do grupo WP.29 da UNECE (organização da ONU responsável pelos transportes) adotada em 2020 [2] e que exige uma série de requisitos mínimos de segurança em carros novos homologados a partir de 2022. Um dos pontos abordados na legislação é a necessidade de uma gestão eficaz das chaves de encriptação, não reutilizando as mesmas chaves através de veículos diferentes e funções diferentes. Construir um sistema eficaz é um grande desafio, uma vez que o volume de carros, a necessidade de manter o suporte para esses carros e seus sistemas conectados por até 20 anos após a venda e o número de funções que exigem chaves criptográficas crescendo exponencialmente, o custo adicionado às limitações de processamento das centrais eletrônicas e limitação de largura de banda na comunicação torna o uso de soluções de mercado (por exemplo, PKIs convencionais) muito difícil de ser aplicado. Além disso, o atual processo de produção dos veículos foi construído e evoluído em cima de conceitos puramente mecânicos, com foco no tempo de produção e redução de custos. Isso traz um desafio extra para a implantação de sistemas conectados aos módulos eletrônicos que demandam tempo para parametrização e profissionais qualificados para sua operação e mitigação de falhas.

Diversas áreas da segurança cibernética passam a ter o foco da engenharia das montadoras pela primeira vez. Neste trabalho trataremos de uma dessas áreas, que atualmente é fundamental para o funcionamento de muitas das funções conectadas e tem sido foco de atenção dos engenheiros. Como apontado anteriormente, lidar com um sistema crítico de segurança, composto por inúmeros nós de rede que possuem diferentes gerações de tecnologia, é extremamente desafiador. Alguns desses nós, chamados ECUs, são mais frequentemente renovados porque fazem parte das áreas da

eletrônica veicular que têm um ciclo de vida mais curto para o lançamento de novos produtos. Podemos destacar os módulos que possuem função de rádio e navegação, com conexão celular, que devem ser atualizados junto com as gerações de telefonia (por exemplo, 3G, 4G e 5G). Outros módulos possuem interface com os usuários dos carros e devem seguir as tendências de design, interação homem-máquina como telas sensíveis ao toque mais sofisticadas, conexão com os smartphones e outros dispositivos móveis. Essa vida útil mais curta do produto acaba resultando em uma atualização constante das versões da plataforma de *hardware* e do sistema operacional, o que, por sua vez, também permite a implementação de controles de segurança modernos. No entanto, o mesmo não pode ser dito em módulos com funções muito específicas, como o controle de uma injeção eletrônica para motores de combustão, ou módulos de controle para portas, freios e etc. Esses módulos podem manter a mesma plataforma de *hardware* por décadas e, mesmo quando atualizados, o fator custo devido ao alto volume de carros vendidos é muito importante. Assim, a capacidade desses módulos de realizar operações necessárias para a implementação de controles de segurança torna-se bastante reduzida.

1.2 - Motivação

Um importante caso de uso, que motivou este trabalho, é quando um desses módulos com limitação de recursos computacionais, mencionado durante a seção anterior, necessita realizar a verificação de um certificado criptográfico para a autenticação de um comando e sua consequente execução. Encontramos exemplos disso olhando para funções como a autenticação de um dispositivo de reparo para um diagnóstico intrusivo pelo conector OBD [Serviço de UDS 0x29] – ISO 14229-1:2020 [3] ou o sistema de carregamento de um veículo elétrico com autenticação do usuário para pagamento da carga feita pela própria conexão entre o veículo e a estação de carregamento PnC ISO 15118:2019 [4]. Estas poderiam ser funções normais para um computador ou smartphone moderno, mas não para os módulos atualmente incorporados em veículos que até então realizavam carregamento de veículos ou diagnóstico de defeitos sem se preocupar com a segurança. Isso não é mais o caso, como vemos na tendência atual de aumento de ataques cibernéticos por esses vetores, como

mostrado no artigo *EV charger attacks trend, Upstream* (2023) [5]. Um ponto simples que mostra a limitação desses módulos para a realização da autenticação do sistema é a própria ausência da informação de tempo (relógio) para verificar se o certificado está dentro do seu prazo de validade. Esses módulos têm *hardware* muito limitado, muitas vezes sem a capacidade de armazenar e gerenciar as informações de tempo. A implantação de um *Sistema de Informação de Tempo* através da rede de informação veicular poderia ser a saída mais óbvia para o problema. No entanto, como garantir que essas informações cheguem ao módulo de forma segura, seja pela manipulação de um invasor na rede ou até mesmo no próprio módulo? Este é o objetivo principal deste trabalho, entender melhor como o problema do tempo afeta um sistema de gerenciamento de chaves criptográficas em geral, como esse problema é gerenciado em um ambiente informático convencional, se essas práticas poderiam ser aplicadas ao universo embarcado automotivo e, finalmente, se não, como podemos propor um modelo que atenda às necessidades atuais aqui apresentadas.

1.3 - Estrutura do Documento

A partir da conexão apresentada e da motivação para o desenvolvimento de uma pesquisa dentro da área de interesse, este documento de dissertação está estruturado da seguinte forma:

O capítulo 2*, Referencial Teórico,* é a espinha dorsal da tese, trazendo uma revisão sistemática da literatura sobre o tema, seguindo as etapas de protocolo de revisão, execução e consequente apresentação dos resultados. O capítulo finaliza com a discussão dos achados, para apresentar quais foram as lacunas encontradas e como este trabalho pretende contribuir para o desenvolvimento dos temas em aberto.

O capítulo 3*, Metodologia,* apresenta a metodologia escolhida para este trabalho de pesquisa, seus fundamentos e etapas e, finalmente, como essa metodologia foi aplicada no desenvolvimento da pesquisa aqui apresentada.

O capítulo 4*, Problemas e Objetivos*, utilizando princípios metodológicos como bússola, apresenta detalhadamente o problema aqui identificado, seus contornos e qual o objetivo desta pesquisa frente ao problema apresentado.

O capítulo 5, *Proposta do Artefato*, traz um dos fundamentos da metodologia de trabalho escolhida que é a identificação, desenvolvimento e implementação de um artefato que permita a proposição de uma solução para o problema identificado. Este capítulo apresenta a partir dos requisitos do artefato, sua proposta, uma visão geral, suas especificações e, finalmente, sua implementação.

Por fim, o capítulo 6*, Demonstração, Avaliação e Conclusões*, traz inicialmente a demonstração da execução do artefato, para validar que ele é funcional e permitirá avançar nas análises. Em seguida apresenta os testes realizados em casos de uso escolhidos que permitiram a coleta de dados para orientar a avaliação da eficácia do artefato em apresentar uma solução para o problema identificado. Finalmente apresenta as considerações sobre os dados encontrados durante os testes, para demonstrar o comportamento do artefato, quais são as contribuições finais do trabalho em relação ao que foi efetivo para a solução do problema, mas também apresenta as limitações da solução proposta, que servem de base para futuros projetos no tema escolhido.

Capítulo 2
Referencial Teórico

2.1 - Revisão da Literatura

Uma revisão sistemática da literatura é de suma importância para uma dissertação de mestrado, especialmente na área da informática. Ela fornece uma abordagem abrangente e rigorosa para identificar, avaliar e sintetizar pesquisas existentes em uma área específica de interesse. Ao conduzir uma revisão sistemática, os pesquisadores podem obter uma compreensão profunda do estado atual do conhecimento, identificar lacunas de pesquisa e desenvolver uma forte base teórica para seu trabalho. No campo da informática, onde os avanços ocorrem rapidamente, uma revisão sistemática da literatura ajuda os pesquisadores a se manterem atualizados com as últimas tendências e descobertas da pesquisa. Permite a identificação de melhores práticas, metodologias emergentes e áreas potenciais para pesquisas futuras. Além disso, ao adotar uma abordagem sistemática, os pesquisadores podem aumentar a credibilidade e a validade de seus trabalhos, garantindo que seus achados sejam baseados em uma análise robusta e imparcial da literatura existente. De modo geral, a revisão sistemática da literatura é uma ferramenta indispensável para dominar o panorama do conhecimento existente e contribuir significativamente para o campo da informática.

Seguindo o artigo *Guidelines for performing Systematic Literature Reviews in Software Engineering v2.3* (2007) [6] podemos responder algumas perguntas que podem nos ajudar a entender se este trabalho necessita de uma revisão sistemática da literatura. O uso de uma abordagem de revisão sistemática da literatura é essencial para uma dissertação focada na compreensão das soluções necessárias para proteger as informações de tempo dentro da arquitetura do veículo para validar certificados. A disponibilidade limitada de estudos específicos sobre a segurança de informações sobre tempo e validação de certificados no contexto da arquitetura de veículos requer uma revisão sistemática. Por meio da busca e avaliação sistemática da literatura existente, a revisão visa preencher a lacuna de conhecimento e identificar potenciais soluções.

A abordagem de revisão sistemática da literatura permite uma busca abrangente em várias fontes, incluindo bibliotecas digitais, bases de dados acadêmicas com artigos científicos e também literatura cinzenta. Ao procurar em ampla rede de informações,

aumentamos as chances de identificar estudos relevantes que indiretamente abordam o tema ou fornecem *insights* aplicáveis à pergunta de pesquisa.

Os critérios de inclusão e exclusão são meticulosamente definidos para garantir que apenas estudos direta ou tangencialmente relacionados à segurança de informações de tempo e validação de certificados dentro da arquitetura do veículo sejam incluídos. Esse processo rigoroso ajuda a filtrar estudos que não estão intimamente alinhados com os objetivos da pesquisa, aumentando a precisão e a relevância da revisão.

Ao avaliar criticamente a qualidade dos estudos selecionados, a revisão garante que os achados sejam baseados em pesquisas confiáveis e robustas. Os critérios de avaliação da qualidade visam avaliar o rigor metodológico, a validade e a confiabilidade dos estudos incluídos, aumentando a credibilidade dos achados sintetizados.

A abordagem sistemática empregada na extração de dados garante que todas as informações relevantes dos estudos primários sejam capturadas de forma consistente. Isso permite uma análise e síntese abrangente dos dados, possibilitando uma compreensão mais profunda do tema e a identificação de possíveis soluções.

Por meio da síntese dos dados extraídos, a revisão visa descobrir temas, padrões e possíveis soluções comuns para proteger informações de tempo e validar certificados dentro da arquitetura do veículo. Essa análise sistemática proporciona uma visão holística da literatura existente, mesmo na ausência de estudos específicos, possibilitando a identificação de estratégias e práticas efetivas.

Em conclusão, a abordagem de revisão sistemática da literatura é essencial para a dissertação, pois aborda a falta de estudos específicos sobre segurança de informações de tempo e validação de certificados dentro da arquitetura veicular. Por meio da busca, avaliação e síntese sistemática da literatura disponível, a revisão visa proporcionar uma compreensão abrangente do tema e identificar soluções efetivas, contribuindo para o avanço do conhecimento nessa área.

2.1.1 - Protocolo

Como primeiro passo após o planejamento da revisão sistemática da literatura, faz-se necessária a definição do protocolo que será utilizado para realizar a extensa busca. Abaixo passo a definir o protocolo a ser utilizado.

Como contexto, temo o uso crescente de certificados digitais na indústria automotiva levanta a necessidade de uma gestão eficaz da expiração do certificado. Garantir a verificação segura e oportuna da validade do certificado é crucial para manter a integridade dos principais sistemas de gerenciamento. Esta revisão sistemática da literatura tem como objetivo explorar as abordagens e estratégias existentes para gerenciar o tempo na verificação da expiração de certificados, com foco na segurança da informação na indústria automotiva ou em outros sistemas críticos de segurança que possam ser reutilizados.

Durante a fase de seleção do tema para essa tese, refletimos sobre o fato do tipo de problema aqui levantado ser algo comum em outras áreas da informática e o entendimento de ainda ser um problema no campo automotivo, sendo assim, definimos as questões a serem utilizadas durante a pesquisa, de maneira a esclarecer se isso é ainda realmente um problema e qual o atual estado da arte. Como questão principal temos:

- Quais são as técnicas e abordagens existentes para o gerenciamento de *timestamp* em certificados criptográficos em automóveis ou outros sistemas críticos de segurança que podem ser reutilizados?

Como questões secundárias para o suporte da pesquisa, temos:

- Quais são os desafios associados ao gerenciamento do tempo para verificação de expiração de certificados na indústria automotiva (ou outros sistemas embarcados críticos de segurança)?
- Que estratégias e técnicas têm sido propostas na literatura para enfrentar esses desafios?
- Quais são as melhores práticas para garantir a segurança e a integridade da verificação de validade de certificados em sistemas de gerenciamento de

chaves dentro da indústria automotiva (ou outros sistemas embarcados críticos de segurança, como aeronaves, trens, máquinas agrícolas e etc)?

A estratégia de busca de estudos primários é verificar bibliotecas digitais para artigos científicos e literatura cinzenta que são relevantes para sistemas críticos de segurança como os automotivos (por exemplo, IEEE, SAE, ESCAR e etc). Os termos de pesquisa incluirão combinações de palavras-chave, como "*time management*," "*secure time*," "*secure clock*," "*authenticated time*," "*time sharing,*" "*central time sourcing*," "*certificate expiration verification*," "*key management*," "*information security*," "*automotive industry*," "*vehicle electrical architecture*," e termos relacionados.

O próximo passo é a definição dos critérios de seleção dos estudos. A tabela abaixo apresenta os critérios definidos no protocolo de inclusão e exclusão do material a ser selecionado. Importante ressaltar que mesmo com estudos relacionados à área de informática terem um tempo de validade em termos de relevância entre 5 e 6 anos, utilizaremos um critério de inclusão de 10 anos levando em conta o ciclo de desenvolvimento lento de um veículo, que leva cerca de 5 anos para o seu lançamento e de 15 a 20 anos de vida pós lançamento incluindo adição de novas funcionalidades e manutenção. O quadro abaixo apresenta os critérios de seleção:

Critérios de inclusão	Critérios de exclusão
Artigos científicos e literatura cinzenta que abordam diretamente o gerenciamento de *timestamp* para certificados criptográficos em automóveis ou outros sistemas embarcados críticos de segurança (como aeronaves, trens, máquinas agrícolas, rede industrial com sensores e atuadores).	Estudos que não se concentram especificamente no gerenciamento de *timestamp* para certificados criptográficos em automóveis ou outros sistemas embarcados críticos de segurança (como a rede de TI tradicional pura, onde o poder de processamento, a latência e a largura de banda não são um problema).
Publicações nos últimos 10 anos para garantir atualidade e relevância.	Publicações com mais de 10 anos que podem não refletir práticas e tecnologias atuais.
Estudos apresentando técnicas, estratégias, soluções ou melhores práticas relacionadas ao gerenciamento de tempo em sistemas de gerenciamento de chaves para verificação de expiração de certificados.	Documentos não científicos, como relatórios de mercado, artigos de imprensa e postagens em blogs.

Tabela 1 - Critérios de seleção

Uma lista de verificação e o procedimento de avaliação da qualidade do estudo é apresentada a seguir, de maneira a avaliar a qualidade e a confiabilidade dos estudos primários no contexto de tempo seguro para validação da certificados em sistemas críticos de segurança. Essas verificações ajudam a garantir a inclusão de estudos de alta qualidade na revisão sistemática da literatura:

	Desenho do estudo	Faixa de pontuação	Pontuação de corte
1	O desenho do estudo é adequado para abordar a questão de pesquisa?	1-5	<3
2	O estudo emprega uma metodologia rigorosa para investigar o tempo seguro para validação da certificados?	1-5	<3
3	Os métodos de coleta de dados estão claramente descritos e adequados aos objetivos da pesquisa?	1-5	<3
4	O estudo inclui um grupo controle ou referência comparável para comparação, se aplicável?	1-5	<3

Tabela 2 - Avaliação do Desenho do Estudo

	Tamanho e Seleção da Amostra	Faixa de pontuação	Pontuação de corte
1	O tamanho da amostra é adequado para tirar conclusões significativas?	1-5	<3
2	O método de amostragem está claramente descrito e é apropriado para o contexto da pesquisa?	1-5	<3
3	Os critérios de inclusão e exclusão para a seleção dos participantes estão claramente indicados?	1-5	<3
4	Há uma descrição clara das características da população estudada?	1-5	<3

Tabela 3 - Tamanho da Amostra e Avaliação da Seleção

	Coleta e Análise dos Dados	Faixa de pontuação	Pontuação de corte
1	Os procedimentos de coleta de dados são bem definidos e replicáveis?	1-5	<3
2	Os métodos de análise dos dados são apropriados para a questão de pesquisa e para os dados coletados?	1-5	<3
3	As análises estatísticas estão adequadamente descritas, incluindo medidas de tendência central, variabilidade e significância estatística, quando aplicável?	1-5	<3
4	Quaisquer suposições feitas durante a análise dos dados são claramente declaradas e justificadas?	1-5	<3

Tabela 4 - Avaliação da Coleta e Análise de Dados

	Validade e Confiabilidade	Faixa de pontuação	Pontuação de corte
1	O estudo aborda potenciais vieses e fatores de confusão?	1-5	<3
2	Os instrumentos e ferramentas de medição são validados e confiáveis?	1-5	<3
3	Existem medidas tomadas para garantir a validade interna e externa do estudo?	1-5	<3
4	Os achados são consistentes com os objetivos do estudo e com a questão de pesquisa?	1-5	<3

Tabela 5 - Avaliação da Validade e Confiabilidade

	Considerações Éticas	Faixa de pontuação	Pontuação de corte
1	O estudo segue as diretrizes éticas e obtém as aprovações éticas necessárias, se aplicável?	1-5	<3
2	Os direitos e a privacidade dos participantes estão protegidos?	1-5	<3
3	Existe uma declaração clara de consentimento informado e participação voluntária?	1-5	<3

Tabela 6 - Avaliação da Considerações Éticas

	Relatórios e Documentação	Faixa de pontuação	Pontuação de corte
1	O relatório do estudo é claro, bem-organizado e estruturado?	1-5	<3
2	O estudo fornece detalhes suficientes para permitir a replicação ou uma análise mais aprofundada?	1-5	<3
3	Limitações e potenciais fontes de viés são reconhecidas e discutidas?	1-5	<3
4	As conclusões são apoiadas pelos resultados e dados do estudo?	1-5	<3

Tabela 7 - Avaliação dos Relatórios e Documentação

O processo que de revisão sistemática da literatura foi realizado seguindo o seguinte fluxo:

- Uma compreensão clara sobre a lista de verificação de avaliação da qualidade do estudo e os critérios descritos acima.
- Aplicar a lista de verificação a cada estudo primário selecionado.
- Avaliar cada critério para cada estudo de forma independente, fornecendo uma pontuação ou classificação com base no grau de realização.
- Determinar um limiar ou pontuação mínima para inclusão no estudo com base na avaliação geral da qualidade.
- Em casos de discordância ou incerteza, consultar o professor orientador.
- Documentar o processo de avaliação da qualidade, incluindo as pontuações ou classificações atribuídas a cada estudo, para garantir a transparência e a reprodutibilidade.

Com a aplicação da lista de verificação e do procedimento de avaliação da qualidade deste estudo, foi possível garantir que os estudos primários selecionados para a revisão sistemática da literatura tivessem alta qualidade, fossem confiáveis e contribuíssem para a compreensão do tempo seguro para validação de certificados em sistemas críticos de segurança, como automóveis, aeronaves, máquinas agrícolas e domínios similares.

Como estratégia de extração de dados, um formulário padronizado foi criado para coletar informações relevantes de cada estudo primário. O protocolo especifica os elementos de dados necessários.

Os dados relevantes dos artigos selecionados foram extraídos e organizados de acordo com os seguintes aspectos:

1 - Autor(es) e ano de publicação.

2 - Objetivo(s) do estudo.

3 - Sistema alvo (por exemplo, automotivo, aeronave, trem, IoT, etc).

4 - Métodos e técnicas empregadas.

5 - Resultados e principais conclusões.

A estratégia de síntese foi realizada para identificar padrões, tendências e lacunas na literatura relacionadas ao gerenciamento de *timestamp* para certificados criptográficos em automóveis. Seguindo o padrão estabelecido pelo item anterior sobre extração de dados, a síntese deveria trazer além dos itens anteriores os principais *insights*, lacunas identificadas quando aplicadas ao ambiente automotivo e as áreas destacadas como potenciais pesquisas futuras.

Nenhuma meta-análise formal é pretendida.

Os resultados da revisão sistemática da literatura serão divulgados por meio dessa dissertação de mestrado e, se apropriado, a divulgação adicional poderá incluir apresentações em congressos ou publicação em periódicos relevantes, definindo assim a estratégia de disseminação.

2.1.2 - Execução

Seguindo com a revisão sistemática da literatura, passamos para a execução do protocolo definido na seção anterior. Isso se deveu, principalmente, à busca de material científico em fontes confiáveis. Abaixo listo as bases de dados consultadas:

- https://ieeexplore.ieee.org/
- https://dl.acm.org/
- https://www.usenix.org/
- https://www.elsevier.com/
- https://www.ebsco.com/
- https://link.springer.com/
- https://www.sciencedirect.com/

Para a realização da busca, foram utilizadas as ferramentas *Google Advanced Search, Google Scholar* e *Connected Papers* com as configurações apropriadas, utilizando-se as palavras-chave de busca definidas. Embora os instrumentos tenham sido utilizados como ferramentas de pesquisa, foram utilizados apenas materiais das fontes confiáveis listadas acima.

	Paper: Time-predictable End-system Design for Real-Time Communication	Pontuação	Nota de corte
	Desenho do Estudo	4	<3
1	O desenho do estudo é adequado para abordar a questão de pesquisa?	4	<3
2	O estudo emprega uma metodologia rigorosa para investigar o tempo seguro para validação da certificados?	4	<3
3	Os métodos de coleta de dados estão claramente descritos e adequados aos objetivos da pesquisa?	4	<3
4	O estudo inclui um grupo controle ou referência comparável para comparação, se aplicável?	NA	<3
	Tamanho e Seleção da Amostra	NA	<3
1	O tamanho da amostra é adequado para tirar conclusões significativas?		<3
2	O método de amostragem está claramente descrito e é apropriado para o contexto da pesquisa?		<3
3	Os critérios de inclusão e exclusão para a seleção dos participantes estão claramente indicados?		<3
4	Há uma descrição clara das características da população estudada?		<3
	Coleta e Análise dos Dados	4	<3
1	Os procedimentos de coleta de dados são bem definidos e replicáveis?	4	<3
2	Os métodos de análise dos dados são apropriados para a questão de pesquisa e para os dados coletados?	3	<3
3	As análises estatísticas estão adequadamente descritas, incluindo medidas de tendência central, variabilidade e significância estatística, quando aplicável?	4	<3
4	Quaisquer suposições feitas durante a análise dos dados são claramente declaradas e justificadas?	3	<3
	Validade e Confiabilidade	4	<3
1	O estudo aborda potenciais vieses e fatores de confusão?	4	<3
2	Os instrumentos e ferramentas de medição são validados e confiáveis?	3	<3
3	Existem medidas tomadas para garantir a validade interna e externa do estudo?	3	<3
4	Os achados são consistentes com os objetivos do estudo e com a questão de pesquisa?	4	<3
	Considerações Éticas	NA	<3
1	O estudo segue as diretrizes éticas e obtém as aprovações éticas necessárias, se aplicável?		<3
2	Os direitos e a privacidade dos participantes estão protegidos?		<3
3	Existe uma declaração clara de consentimento informado e participação voluntária?		<3
	Relatórios e Documentação	4	<3
1	O relatório do estudo é claro, bem-organizado e estruturado?	4	<3
2	O estudo fornece detalhes suficientes para permitir a replicação ou uma análise mais aprofundada?	4	<3
3	Limitações e potenciais fontes de viés são reconhecidas e discutidas?	3	<3
4	As conclusões são apoiadas pelos resultados e dados do estudo?	4	<3

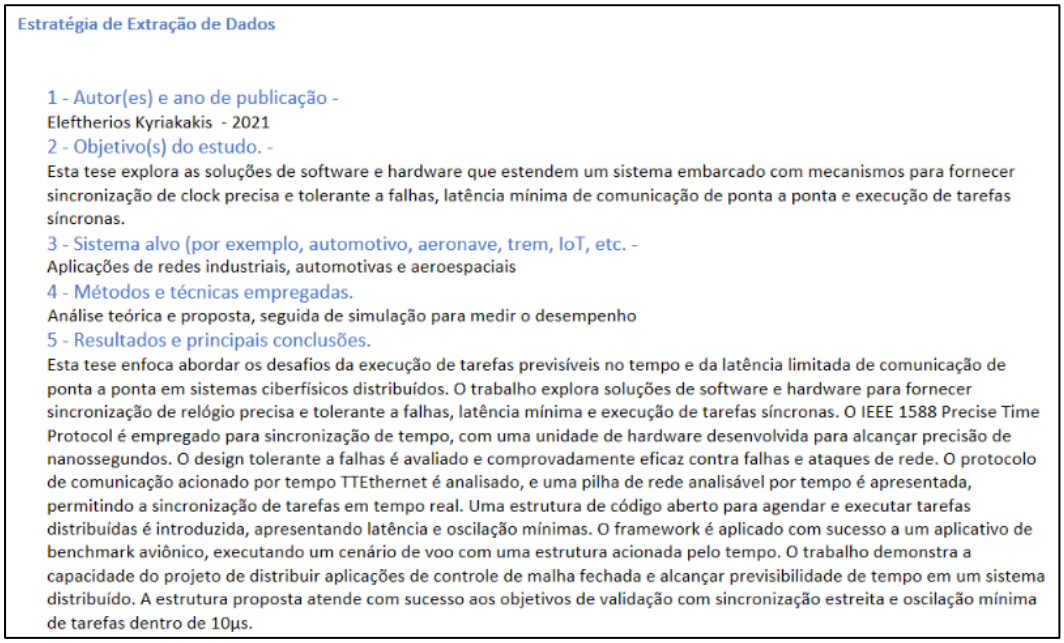
Figura 1 - Exemplo da aplicação da avaliação da qualidade do estudo

Em seguida, aplicando-se os critérios de inclusão e exclusão, foram encontrados **138** artigos, dissertações, teses e publicações científicas para posterior análise. Após a aplicação dos critérios de inclusão e exclusão, um total de **54** itens foi considerado adequado para análise posterior. Por fim, **40** itens foram selecionados com base em sua pontuação de qualidade atribuída.

Para facilitar a execução da próxima etapa do protocolo, os materiais encontrados foram categorizados em "Propostas de Projeto de Arquitetura Segura", "Propostas de Mecanismos de Gerenciamento de Chaves Criptográficas" e "Propostas de Sincronização Segura de Tempo". Cada categoria passou, então, pela próxima etapa do protocolo, que é

a análise adequada da qualidade do material, a fim de receber uma pontuação para cada item em avaliação.

Apenas os estudos em que nenhum item aplicável recebeu uma pontuação menor que 3, passaram para a próxima fase do protocolo, que é a extração dos dados. Na figura abaixo vemos um exemplo de como os dados foram extraídos de cada estudo de forma harmônica, seguindo o protocolo:


Estratégia de Extração de Dados

1 - Autor(es) e ano de publicação -
Eleftherios Kyriakakis - 2021
2 - Objetivo(s) do estudo. -
Esta tese explora as soluções de software e hardware que estendem um sistema embarcado com mecanismos para fornecer sincronização de clock precisa e tolerante a falhas, latência mínima de comunicação de ponta a ponta e execução de tarefas síncronas.
3 - Sistema alvo (por exemplo, automotivo, aeronave, trem, IoT, etc. -
Aplicações de redes industriais, automotivas e aeroespaciais
4 - Métodos e técnicas empregadas.
Análise teórica e proposta, seguida de simulação para medir o desempenho
5 - Resultados e principais conclusões.
Esta tese enfoca abordar os desafios da execução de tarefas previsíveis no tempo e da latência limitada de comunicação de ponta a ponta em sistemas ciberfísicos distribuídos. O trabalho explora soluções de software e hardware para fornecer sincronização de relógio precisa e tolerante a falhas, latência mínima e execução de tarefas síncronas. O IEEE 1588 Precise Time Protocol é empregado para sincronização de tempo, com uma unidade de hardware desenvolvida para alcançar precisão de nanossegundos. O design tolerante a falhas é avaliado e comprovadamente eficaz contra falhas e ataques de rede. O protocolo de comunicação acionado por tempo TTEthernet é analisado, e uma pilha de rede analisável por tempo é apresentada, permitindo a sincronização de tarefas em tempo real. Uma estrutura de código aberto para agendar e executar tarefas distribuídas é introduzida, apresentando latência e oscilação mínimas. O framework é aplicado com sucesso a um aplicativo de benchmark aviônico, executando um cenário de voo com uma estrutura acionada pelo tempo. O trabalho demonstra a capacidade do projeto de distribuir aplicações de controle de malha fechada e alcançar previsibilidade de tempo em um sistema distribuído. A estrutura proposta atende com sucesso aos objetivos de validação com sincronização estreita e oscilação mínima de tarefas dentro de 10µs.

Figura 2 - Exemplo de extração de dados de estudos qualificados

Após a extração dos dados, passa-se para a última fase de análise individual dos estudos que se refere à consolidação dos dados extraídos em forma de síntese, conforme exemplo mostrado na figura 3.

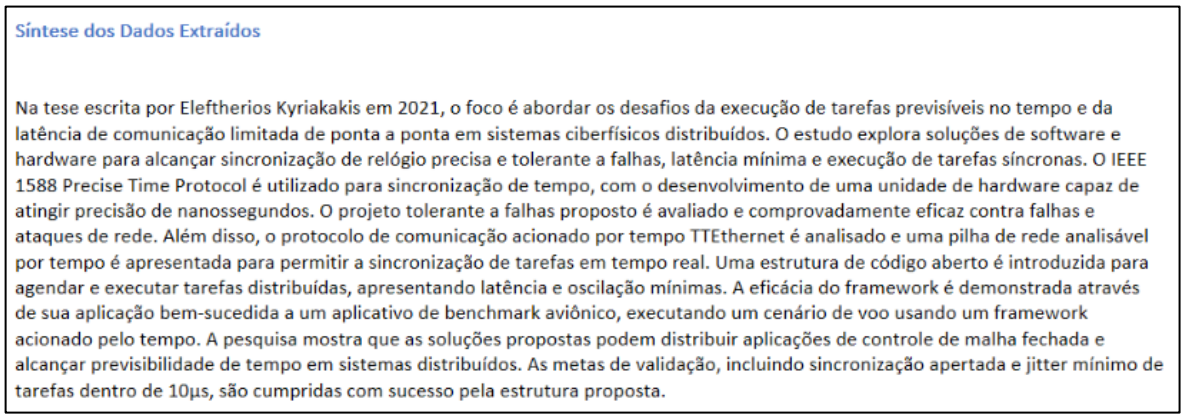
A seguir apresentaremos a síntese de todos os estudos qualificados, de forma estruturada, para a construção do estado da arte na próxima seção. A sequência apresentada tem como objetivo construir o estado da arte criando uma visão consolidada seguindo três etapas:

1 - Começamos com projetos de arquitetura segura propostos a partir de sistemas automotivos ou relacionados a partir de uma perspectiva de tempo seguro.

2 - Em seguida, vamos a uma análise da necessária relação de confiança entre as entidades, que deve ser construída por um esquema eficaz de Gestão de Chaves de

Criptografia.

3 - Por fim, analisaremos os achados relevantes da Sincronização Segura de Tempo Seguro, podendo agora definir nosso estado da arte e suas lacunas.


Síntese dos Dados Extraídos

Na tese escrita por Eleftherios Kyriakakis em 2021, o foco é abordar os desafios da execução de tarefas previsíveis no tempo e da latência de comunicação limitada de ponta a ponta em sistemas ciberfísicos distribuídos. O estudo explora soluções de software e hardware para alcançar sincronização de relógio precisa e tolerante a falhas, latência mínima e execução de tarefas síncronas. O IEEE 1588 Precise Time Protocol é utilizado para sincronização de tempo, com o desenvolvimento de uma unidade de hardware capaz de atingir precisão de nanossegundos. O projeto tolerante a falhas proposto é avaliado e comprovadamente eficaz contra falhas e ataques de rede. Além disso, o protocolo de comunicação acionado por tempo TTEthernet é analisado e uma pilha de rede analisável por tempo é apresentada para permitir a sincronização de tarefas em tempo real. Uma estrutura de código aberto é introduzida para agendar e executar tarefas distribuídas, apresentando latência e oscilação mínimas. A eficácia do framework é demonstrada através de sua aplicação bem-sucedida a um aplicativo de benchmark aviônico, executando um cenário de voo usando um framework acionado pelo tempo. A pesquisa mostra que as soluções propostas podem distribuir aplicações de controle de malha fechada e alcançar previsibilidade de tempo em sistemas distribuídos. As metas de validação, incluindo sincronização apertada e jitter mínimo de tarefas dentro de 10µs, são cumpridas com sucesso pela estrutura proposta.

Figura 3 - Exemplo de síntese de dados extraídos de estudos selecionados

Propostas de Projeto de Arquitetura Segura

Iniciando a revisão agrupando o material que passou no filtro de qualidade sob o tema de propostas de projeto de arquitetura segura, podemos trazer inicialmente uma visão genérica em torno do tópico principal de gerenciamento seguro de tempo.

Arquitetura Segura Genérica para Gerenciamento de Tempo

Os autores Anwar e Srivastava (2020) [7] apresentaram uma nova arquitetura de sincronização de relógio projetada para neutralizar ataques de transferência de tempo, que pode manipular informações de tempo trocadas entre um mestre e um cliente em sistemas distribuídos. A arquitetura aproveita um controle *feedforward* com um mecanismo de ajuste de *clock "feedback trim-based"*. Essa abordagem separa os cálculos de tempo e frequência, usando pacotes unidirecionais para calcular o erro de frequência relativa e pacotes bidirecionais para calcular o erro de deslocamento. A arquitetura também emprega técnicas de filtragem de pacotes para restaurar a periodicidade de pacotes com atraso variável e para localizar pacotes sem atrasos, fornecendo estimativas

precisas de deslocamento. Além disso, a arquitetura inclui um modelador de frequência que ajusta a frequência relativa com base no deslocamento para sincronizar o relógio. Os autores aplicaram sua arquitetura ao protocolo *Precision Time Protocol* (PTP), que será um protocolo recorrente sob o tópico aqui analisado, e avaliaram em um *testbed* suportado por *hardware* sob vários cenários de ataque de atraso. Os autores demonstraram a capacidade de sua arquitetura de alcançar a sintonização e sincronização do relógio em diferentes cenários de ataque de atraso e limitar os erros de relógio diante de um poderoso invasor de rede. Eles também discutem as limitações potenciais e as direções de trabalho futuras, incluindo a extensão de sua arquitetura para outros protocolos, a abordagem de padrões de atraso mais complexos e a incorporação de mecanismos de segurança. Seu artigo oferece uma estratégia nova e eficiente para mitigar ataques de transferência de tempo, muitas vezes percebidos como poderosos demais para serem efetivamente protegidos. O artigo também propõem melhorias importantes para o protocolo PTP, mas destaca o desafio de redesenho das arquiteturas vigentes.

O estudo de Ran Canetti et al. (2017) [8], aprofunda a importância da sincronização de tempo precisa para proteger sistemas distribuídos. Eles chamam a atenção para a dependência de vários sistemas do mundo real, como comunicação pela Internet e revogação de certificados, da capacidade dos participantes de determinar e manter com precisão as medições de tempo. No entanto, casos recentes de ataques expuseram vulnerabilidades em protocolos de tempo padrão, aumentando assim os riscos de segurança. A falta de soluções de segurança robustas para protocolos de tempo de rede agrava ainda mais o desafio de garantir segurança em tempo real para aplicativos. Em resposta a essas questões, os autores introduzem controles de segurança dentro do *framework* de segurança *universally composable* (UC). Eles elaboram funcionalidades ideais que encapsulam formas comuns de medição de tempo em sistemas contemporâneos. Seu estudo ilustra como essas funcionalidades podem ser atualizadas por protocolos do mundo real e empregadas para proteger aplicativos dependentes do tempo, com foco específico em certificados com tempos de revogação e expiração. Esta metodologia promove uma abordagem transparente e modular para o

consenso temporal em sistemas sensíveis à segurança. O estudo situa sua modelagem e análise dentro do *framework* UC, aproveitando sua natureza assíncrona e orientada a eventos. Isso permite a integração de considerações em tempo real no trabalho analítico que já foi feito dentro do *framework*. É importante ressaltar que ele auxilia a assimilação rigorosa de aspectos em tempo real em ferramentas criptográficas e suas primitivas. É um estudo promissor, mas mais trabalhos são necessários para evoluir o tema.

S. N. A. Ahmed (2018) [9] propõe um novo método para melhorar o desempenho de sincronização de sistemas de comunicação baseados em *frames* em ambientes complexos. O método proposto é baseado em um algoritmo de correlação cruzada segmentado que é mais robusto para deslocamentos de frequência portadora e operando em ambientes de alta mobilidade do que o algoritmo de correlação cruzada convencional. O método proposto também se mostrou mais eficiente em termos de consumo de energia e recursos de *hardware*. O artigo começa discutindo a importância da sincronização em sistemas de comunicação baseados em *frames*. A sincronização é essencial para uma comunicação confiável, pois permite que o transmissor e o receptor concordem sobre o tempo e a frequência do sinal transmitido. No entanto, a sincronização pode ser difícil de alcançar em ambientes complexos, como quando o transmissor e o receptor estão se movendo em altas velocidades ou quando há muito ruído e interferência. Em seguida, o artigo apresenta o método proposto para melhorar o desempenho da sincronização. O método proposto é baseado em um algoritmo de correlação cruzada segmentada que divide o sinal recebido em blocos menores e realiza a correlação cruzada entre cada bloco e uma réplica local do preâmbulo. Isso ajuda a reduzir os efeitos de ruído e interferência, e torna o algoritmo mais robusto para deslocamentos de frequência portadora. O método proposto também tem se mostrado mais eficiente em termos de consumo de energia e recursos de *hardware*, pois requer apenas uma fração do número de operações como o algoritmo convencional de correlação cruzada. Em seguida, o artigo apresenta os resultados de estudos de simulação que avaliam o desempenho do método proposto. Os estudos de simulação mostram que o método proposto alcança um bom desempenho de sincronização em ambientes desafiadores, como quando há grandes deslocamentos de frequência portadora ou

deslocamentos Doppler. O método proposto também consome menos energia e usa menos recursos de *hardware* do que o algoritmo de correlação cruzada convencional. No geral, o artigo apresenta um novo método promissor para melhorar o desempenho de sincronização de sistemas de comunicação baseados em quadros em ambientes complexos. O método proposto é eficiente, escalável e robusto, e tem demonstrado um bom desempenho de sincronização em estudos de simulação.

Aqui estão algumas das principais conclusões do artigo:

· O método proposto é mais robusto para deslocamentos de frequência portadora e operando em ambientes de alta mobilidade do que o algoritmo convencional de correlação cruzada.

· A arquitetura proposta é eficiente em termos de consumo de energia e recursos de *hardware*.

· O método proposto alcança um bom desempenho de sincronização nas simulações realizadas.

· O método proposto é uma abordagem promissora para melhorar o desempenho de sincronização de sistemas de comunicação baseados em *frames* em ambientes complexos.

Como o artigo anterior, é um trabalho contínuo que exigirá mais interações para ter uma solução consolidada.

Desafios da arquitetura automotiva

Voltando nossa atenção para o ambiente automotivo, P. Mundhenk (2017) [10] discute os desafios de segurança colocados pela crescente conectividade das arquiteturas E/E (eletro-eletrônicas) automotivas. Propõe três mecanismos de segurança principais para enfrentar estes desafios:

· Um *framework* de análise de segurança em tempo para o design de arquiteturas E/E: esse *framework* ajuda a identificar vulnerabilidades de segurança em arquiteturas E/E durante a fase de projeto.

· Um *framework* de autenticação e autorização de tempo de execução para sistemas E/E: esse *framework* garante que apenas entidades autorizadas possam acessar os sistemas E/E.

· Um esquema de programação flexível para o FlexRay: Este esquema ajuda a melhorar a segurança do FlexRay, um protocolo de comunicação em tempo real usado em aplicações automotivas.

Em seguida, são apresentados os resultados de estudos de simulação que avaliam o desempenho dos mecanismos de segurança propostos. Os resultados mostram que os mecanismos propostos podem efetivamente melhorar a segurança das arquiteturas E/E. Em geral, o artigo fornece fortes evidências de que os mecanismos de segurança propostos podem ser uma adição valiosa à caixa de ferramentas de segurança para sistemas E/E automotivos. Os mecanismos podem ajudar a melhorar a segurança das arquiteturas E/E e protegê-las de ataques cibernéticos.

Aqui estão algumas das principais conclusões do artigo:

· A crescente conectividade das arquiteturas E/E automotivas as torna mais vulneráveis a ataques cibernéticos.

· Vários mecanismos de segurança podem ser usados para enfrentar os desafios de segurança colocados pelas arquiteturas E/E automotivas.

· Os mecanismos de segurança propostos podem efetivamente melhorar a segurança das arquiteturas E/E.

· Os mecanismos de segurança propostos podem ser uma adição valiosa à caixa de ferramentas de segurança para sistemas E/E automotivos.

O artigo é um recurso valioso para pesquisadores e profissionais interessados em segurança para sistemas de E/E automotivos. Ele fornece uma visão abrangente dos desafios de segurança colocados pelas arquiteturas E/E automotivas e propõe uma série de mecanismos de segurança para enfrentar esses desafios. O artigo também apresenta os resultados de estudos de simulação que avaliam o desempenho dos mecanismos de segurança propostos.

O trabalho de pesquisa conduzido por Mundhenk et al. (2015) [11], apresenta um *framework* único com o objetivo de estabelecer uma conexão entre autenticação segura em redes automotivas e a Internet. Esse *framework* foi projetado para permitir trocas de chaves criptográficas em tempo real com *overhead* reduzido, tornando-a ideal para redes de veículos com recursos limitados. A equipe utiliza uma mistura de criptografia simétrica e assimétrica para garantir uma comunicação segura e facilitar atualizações seguras de chaves criptográficas e *software* durante todo o ciclo de vida do veículo. Eles adaptam protocolos de autenticação para dispositivos móveis e protocolos de autorização para *streams* especificamente para o domínio automotivo. Uma característica notável do *framework* é sua compatibilidade com *multicast* e comunicação *broadcast*, que são predominantes em redes automotivas. Os autores validam a eficácia de seu *framework* leve, demonstrando sua capacidade de estabelecer *streams* de mensagens seguras enquanto aderem aos rigorosos requisitos em tempo real das redes automotivas. É preciso trabalhar mais nessa área para definir uma solução robusta em termos de *safety*.

Em um estudo recente, Berbecaru et al. (2023) [12] examinou ataques de integridade de *software* em *Time Distribution Networks* (TDNs), solução de sincronização de tempo segura utilizada em várias aplicações, incluindo redes 5G. Eles apresentam e experimentam uma solução centrada em computação confiável via TPM 2.0 e atestado remoto por meio do *framework Keylime*, verificando os *daemons* de *software* em dispositivos de tempo a partir de um nó confiável. Seu *testbed* experimental usa dispositivos WR-Z16 personalizados, da Seven Solutions, que utilizam o protocolo WR-PTP para precisão de sincronização de sub nanossegundos. Sua solução proposta efetivamente mitiga três tipos de ataques de integridade de *software* em dispositivos de

tempo – modificação de configuração de *software*, alteração ou substituição de *software* executável e alterações de configuração do receptor GNSS no dispositivo de tempo, tudo sem afetar a precisão ou o desempenho da sincronização de tempo do TDN. Eles postulam que a utilização de TPMs e atestado remoto em TDNs é crucial para identificar ataques não detectados. Esta pesquisa tem implicações para as operadoras de TDN que buscam desenvolver serviços de sincronização de tempo robustos, precisos e seguros para redes 5G e outras aplicações baseadas em tempo. No entanto, destacamos o desafio atual enfrentado pelos ECUs na ponta da rede automotiva que não possuem recursos de *hardware* para operar operações seguras como o TPM utilizado no estudo aqui analisado.

Aprendendo com outras áreas fora do setor automotivo

Explorando agora outras áreas que podem enfrentar limitações automotivas semelhantes, Zhai et al. (2023) [13] investigou o problema dos ataques de atraso de tempo em redes de VANTs, prevalente em contextos militares e civis. Eles modelam exclusivamente esse ataque dentro de redes de UAV, destacando sua natureza distinta, aspecto secreto e potencial destrutivo. Para neutralizar esses ataques, eles propõem o ETD, uma estrutura de detecção eficiente que aproveita recursos relacionados a atrasos em quatro dimensões, classificação de uma classe e clustering K-Means para identificar nós maliciosos que perpetram ataques de atraso de tempo. Eles implementam simulações abrangentes no simulador ONE, demonstrando que o ETD atinge mais de 80% de precisão de detecção e incorre em menos de 2,5% de *overhead* adicional em diferentes configurações de rede UAV e protocolos de roteamento. Eles afirmam que o ETD é a estrutura pioneira com foco em ataques de atraso de tempo em redes UAV, contribuindo significativamente para melhorar sua segurança e confiabilidade.

Propostas de Mecanismos de Gerenciamento de Chaves Criptográficas

Seguindo uma abordagem semelhante à usada durante a seção anterior, começaremos a analisar um sistema genérico, passaremos pelo ambiente automotivo e, em seguida, revisaremos outras áreas que enfrentam desafios semelhantes. O objetivo agora é analisar como a relação de confiança entre as entidades poderia ser alcançada usando o sistema de gerenciamento de chaves criptográficas adequado.

Sistemas Genéricos de Gerenciamento de Chaves para Tempo

Os autores Langer and Bermbach (2022) [14] Aborda as vulnerabilidades de segurança do Precision Time Protocol (PTP) e introduzem o protocolo NTS4PTP emergente. O objetivo do estudo é desenvolver uma solução segura para sincronização de tempo em sistemas que utilizam PTP. O protocolo NTS4PTP, desenvolvido em cooperação com o Subcomitê de Segurança do IEEE, aproveita o protocolo Network Time Security (NTS) e um sistema de gerenciamento de chaves para automatizar a distribuição de parâmetros de segurança. Ele suporta modos PTP comuns e pode ser combinado com NTP (Network Time Protocol) protegido por NTS. O artigo discute a importância da sincronização de tempo, os pontos fracos do padrão PTP atual e a importância do NTS4PTP na proteção de redes PTP, particularmente em ambientes industriais. O protocolo é quase totalmente especificado, e uma implementação de prova de conceito é planejada, oferecendo uma solução abrangente para segurança PTPv2.1 integrada com implementação simplificada usando TLS como um protocolo de *framework*. A solução precisa de mais trabalho, pois o protocolo proposto não está maduro o suficiente para implementação.

Sistemas Automotivos de Gerenciamento de Chaves para Tempo

O estudo de Kent et al. (2020) [15] concentra-se em abordar os riscos de segurança associados a um firmware de um Electronic Control Unit (ECU) no setor automotivo. À medida que os veículos se tornam tecnologicamente mais avançados, com vários ECUs se comunicando por meio de uma arquitetura de rede, garantir a integridade

do firmware é crucial para a segurança do veículo. O artigo propõe uma infraestrutura baseada em chave assimétrica para assinatura e validação de firmware de ECU, alavancando colaborações entre fabricantes automotivos e seus fornecedores (Tier-1). Por meio de análise teórica, proposta e simulação, demonstra-se a viabilidade e a resistência aos ataques. O esquema aumenta a integridade do *firmware* da ECU e pode ser adotado pelos fabricantes para evitar atualizações maliciosas. A adoção de um forte sistema de Infraestrutura de Chave Pública (PKI) no setor automotivo também pode inspirar a implementação de soluções baseadas em PKI em outros aspectos do negócio. No entanto, uma minuciosa análise financeira dos custos envolvidos é necessária para a adoção generalizada do esquema proposto, que pode ser atenuado por avanços em chipsets e *hardware* criptográfico, já disponíveis com custo factível para uso em grandes volumes.

Aprendizados de Outras Áreas para Gerenciamento de Tempo

O artigo "*A Novel Distributed Multiparty Keying Scheme for Mobile and IoT Devices*" de Mahmood et al. (2018) [16] apresenta uma nova abordagem para proteger o gerenciamento de chaves no contexto de dispositivos móveis e IoT. O objetivo do estudo é propor um esquema de chaveamento multipartidário distribuído usando mapas caóticos para *hashing* unidirecional e polinômios de Chebyshev para estabelecer uma chave multipartidária comum. O esquema abrange o chaveamento entre servidores confiáveis, chefes de grupo e dispositivos inteligentes, permitindo o estabelecimento seguro de chaves de sessão e o estabelecimento de chaves entre grupos. A integridade das mensagens é garantida através de funções de *hash* caóticas baseadas em mapas, e os polinômios de Chebyshev facilitam o estabelecimento de chaves e a geração de texto cifrado. A eficácia do esquema é validada por meio de especificação formal, análise de segurança, simulações e um banco de testes. Os resultados demonstram a superioridade do esquema proposto em termos de custo computacional, custo de comunicação e resiliência em relação aos esquemas existentes. O esquema proposto oferece maior eficiência e segurança para o gerenciamento distribuído de chaves em ambientes IoT. A implementação da solução aqui descrita não poderia ser possível para uma rede herdada, encontrada atualmente em veículos em produção.

A dissertação de Cebe (2020) [17] visa abordar o *overhead* gerado por um sistema de gestão de chaves criptográficas, que é um problema para as limitações de sistemas de *Smart Grid*. O trabalho propõe três abordagens para melhorar a segurança e a eficiência na gestão de chaves. A primeira abordagem utiliza um método baseado em DHT com assinaturas ECDSA para gerenciar chaves revogadas de forma eficaz. A segunda abordagem introduz um esquema de gerenciamento de revogação usando acumuladores criptográficos, aumentando a segurança e reduzindo o *overhead*. A terceira solução se concentra na redução do *overhead* na troca de chaves por meio de um mecanismo 0-RTT projetado para comunicação de baixa largura de banda. Essas abordagens demonstram melhorias significativas no uso de recursos, eficiência e segurança. Direções de pesquisa futuras incluem explorar o gerenciamento de revogação distribuída em vários níveis, esquemas de acumuladores aprimorados, otimizar parâmetros de troca de chaves, melhorar a segurança do protocolo DNP3 e melhorar o módulo SA para dispositivos legados. Novamente, a limitação da rede herdada pode ser um problema para a adoção da solução.

Propostas de Sincronização Segura de Tempo

Por fim, analisaremos os materiais relacionados com o principal problema a ser resolvido, o Tempo Seguro e sua Sincronização. A revisão começa analisando a solução *off-board* que garantirá as informações corretas para alimentar o veículo, depois revisa os principais mecanismos e protocolos em uso hoje e, finalmente, considera outras soluções propostas.

Tempo Seguro Off-board

Começando pela fonte *off-board* utilizada para informar o veículo o tempo de forma segura, em sua publicação, Annessi et al. (2017) [18] teve como objetivo encontrar um método seguro e eficiente para sincronização de tempo em comunicação *multicast*. Eles conduziram uma análise completa de ameaças de protocolos de sincronização de tempo em infraestruturas críticas, como telecomunicações, automação industrial,

aviônica e distribuição de energia. Com base em sua análise, eles propuseram um novo conjunto de medidas de segurança para proteger a sincronização de tempo de *multicast*. Medições experimentais mostraram que essas medidas de segurança alcançaram a eficiência computacional e de comunicação desejada sem afetar a precisão dos protocolos de sincronização de tempo. No entanto, o artigo tinha limitações em relação a suposições sobre relações de confiança estabelecidas entre nós e a falta de consideração para a interoperabilidade com diferentes tecnologias de redes embarcadas, tornando a aplicação direta à arquitetura elétrica automotiva desafiadora. A dependência de sinais de GPS como fonte segura também foi questionada. Além disso, a configuração de medição se concentrou na precisão e não abordou desafios específicos do ambiente automotivo, como limitações de largura de banda para implementar completamente o protocolo NTP com seus *payloads* assinados digitalmente. Embora com o bom desempenho demonstrado para o sistema crítico de segurança, a solução carece de uma solução de relação de confiança entre as partes e como compartilhar as informações através de uma rede multi tipo encontrada em um veículo.

Um artigo de Frei et al. (2022) [19] introduzir o G-SINC, um sistema inovador projetado para sincronização de tempo global que contorna a dependência de uma única fonte de tempo de referência, como o GNSS, suscetível a interrupções, mau funcionamento ou ataques. O G-SINC incorpora um algoritmo bizantino tolerante a falhas para harmonizar servidores de tempo primários em vários clusters de rede, cada um com ambientes e políticas de confiança distintos. Além disso, o G-SINC explora a arquitetura SCION com reconhecimento de caminho, que facilita a comunicação segura de vários caminhos, a reversibilidade de caminho e a autenticação leve, com o objetivo de reforçar a precisão, a segurança e a resiliência do processo de sincronização de relógio. Avaliado através de simulações em topologias realísticas entre domínios, o G-SINC demonstra sua capacidade de manter uma sincronização de tempo confiável e precisa, mesmo sob nós maliciosos ou interrupções de relógio de referência. Frei e colegas concluem que o G-SINC representa uma solução prática e econômica para sistemas de infraestrutura crítica que precisam de sincronização de *clock* tolerante a falhas e pode ser implantado como uma extensão compatível com versões anteriores para as arquiteturas atuais de sincronização

de tempo. O G-SINC teve bons resultados iniciais, mas a falta de confiança em torno de uma validação robusta e clareza em torno da interoperabilidade em diferentes países são os principais problemas para aplicação direta no universo automotivo.

Spanghero e Papadimitratos (2023) [20] propõe um método para detectar ataques GNSS que manipulam o tempo e a posição do receptor usando diferentes fontes de tempo. Os autores argumentam que os receptores GNSS civis são vulneráveis a vários tipos de ataques de falsificação que podem comprometer a precisão e a integridade da solução PNT. Os autores sugerem que os receptores GNSS podem aproveitar informações externas para validar o tempo fornecido pelo GNSS em relação a várias referências confiáveis. Os autores apresentam um método que combina servidores de tempo de rede seguros, osciladores de precisão locais e Google Roughtime para fornecer um mecanismo de defesa de várias camadas que pode detectar ataques que induzem até mesmo deslocamentos de tempo pequeno, incluindo ataque *cold start*. Os autores implementam um *testbed* de prova de conceito que pode recriar diferentes cenários de ataque, como a simulação, lift-off e ataque de replay. Os autores avaliam o desempenho de seu método sob várias condições e mostram que seu método pode efetivamente detectar ataques GNSS sem modificar o receptor GNSS ou confiar nas propriedades do sinal. Os autores também discutem a escalabilidade e extensibilidade de seu método para diferentes sistemas GNSS e aplicações. Os autores concluem que aproveitar informações externas para validar o tempo fornecido pelo GNSS é uma maneira viável e eficaz de detectar ataques GNSS e fornecer PNT robusto e seguro. O impacto no *hardware* legado seria o principal problema para implementar esse mecanismo de detecção em um veículo.

O trabalho de pesquisa de Fernandez-Hernandez et. al (2020) [21] propõe um esquema de sincronização de tempo para receptores GNSS usando autenticação com atraso de tempo. Eles adaptam o TESLA (Timed Efficient Stream Loss-tolerant) protocolo para sistemas de comunicação unidirecional como o GNSS, destacando a importância de um tempo de referência independente e limites de incerteza para iniciar o protocolo. Os autores analisam diferentes cenários de inicialização e estabelecem procedimentos de inicialização seguros para evitar falsificação de dados e anomalias. Eles também discutem os aspectos práticos da sincronização de receptores GNSS para aplicações de rede e

aviação, fornecendo insights valiosos. As conclusões deste estudo podem ser aplicadas a outros protocolos de autenticação de dados ou sinais que dependem da divulgação tardia de informações criptográficas.

A publicação do NIST, Instituto Nacional de Padrões e Tecnologia dos EUA, com *"A resilient architecture for the realization and distribution of coordinated universal time to critical infrastructure systems in the United States: Methodologies and recommendations from the national institute of standards and technology"* (2021) [22] aborda o objetivo de fornecer uma arquitetura resiliente para a informação universal de tempo. O estudo se concentra em Sistemas de Infraestrutura Crítica nos Estados Unidos que exigem tempo seguro. Os métodos empregados envolvem padrões rigorosos estabelecidos pelo NIST, que aplica achados teóricos e práticos. O relatório é uma resposta à Seção 4, Parte (i) da Ordem Executiva 13905 de Posição, Navegação e Temporização (PNT), que determina a disponibilidade de uma fonte independente GNSS de Tempo Universal Coordenado (UTC) para dar suporte às necessidades de infraestruturas críticas. A publicação descreve e recomenda métodos técnicos já implementados ou potencialmente implementáveis pelo NIST para atender aos requisitos da Ordem Executiva. O objetivo é estabelecer uma arquitetura resiliente para a realização e distribuição da UTC nos Estados Unidos. O NIST forneceu uma boa solução para padronizar uma solução CNSS em termos de segurança, mas a limitação apenas ao mercado dos EUA é o grande problema.

Mecanismos e Protocolos Consolidados de Tempo Seguro

Iniciando a análise em torno de mecanismos e protocolos consolidados, o TESLA (Timed Efficient Stream Loss-tolerant) poderia ser inicialmente um bom candidato para resolver as limitações de sistemas críticos de segurança. O estudo de Teichel et. al (2018) [23], examinou a vulnerabilidade de protocolos de sincronização de tempo unidirecional utilizando mecanismos semelhantes ao Tesla. O mecanismo unidirecional pode ajudar a lidar com a limitação de largura de banda encontrada em um veículo. Eles desenvolveram uma implementação de *testbed* para simular e avaliar as características de segurança e sincronização desses protocolos. Os testes confirmaram a viabilidade de um ataque

teórico, enfatizando a necessidade de medidas de segurança adicionais. O sistema foi considerado seguro até que a primeira fase do ataque foi bem-sucedida, com uma ocorrência quantificada de maneira clara. Os autores recomendaram o estabelecimento de um protocolo de sincronização de tempo com comunicação unidirecional protegida por TESLA, e sugeriram analisar a aplicabilidade do ataque a outros protocolos existentes ou futuros utilizando TESLA. A ferramenta de análise implementada poderia ser utilizada para este fim. Contramedidas, como trocas periódicas bidirecionais, especialmente no contexto do PTP, foram propostas como medidas efetivas. O artigo também discutiu achados relacionados à aplicação tardia e imediata de compensações medidas e o potencial de comutação dinâmica entre comportamentos com base em ameaças detectadas, sugerindo a consideração desses fatores em novas especificações.

Também, em sua publicação, Kristof Teichel e Gregor Hildermeier (2018) [24] avaliaram os protocolos TESLA para validar a eficácia prática dos ataques. O estudo concentrou-se em redes que usam o protocolo TESLA para sincronização de tempo unidirecional. Os autores implementaram os protocolos e realizaram experimentos para identificar problemas de segurança e vulnerabilidades, especificamente com o *TinySeRSync*. Eles propuseram contramedidas para mitigar os ataques, mas essas contramedidas exigem comunicação bidirecional. Os autores também sugeriram pesquisas futuras para analisar a vulnerabilidade de outros protocolos de sincronização de tempo, explorar contramedidas adicionais e conduzir provas formais da segurança da Tesla na sincronização unidirecional. Os problemas de segurança continuam a ser o principal bloqueador.

O trabalho de Langer et al. (2020) [25] apresentou um vetor de ataque que tem como alvo protocolos de sincronização de tempo de transmissão protegidos por mecanismos semelhantes ao TESLA. Seu objetivo foi propor e avaliar possíveis contramedidas para mitigar essa vulnerabilidade. Eles discutiram o uso do verificador modelo UPPAAL para análise e quantificação de segurança, apresentando os resultados obtidos. Além disso, eles revisaram a suscetibilidade de três protocolos de sincronização de tempo protegidos criptograficamente existentes ao vetor de ataque descoberto. Os autores enfatizaram a importância de realizar análises mais aprofundadas sobre

especificações que utilizam mecanismos semelhantes ao Tesla para garantir a comunicação de sincronização de tempo do tipo *broadcast*. Eles mencionaram especificamente a potencial aplicação do NTS-Secured NTP e o trabalho em andamento para adicionar mecanismos de segurança ao padrão IEEE 1588 (PTP). O uso da transmissão TESLA aborda o que poderia ser bom para uma rede automotiva. No entanto, as vulnerabilidades na abordagem TESLA não são totalmente mitigadas e os recursos de SW e HW necessários na ECU na ponta da rede são os maiores problemas para a sua utilização.

Annessi et al. (2017) [26] enfrenta o desafio da autenticação de origem de dados em protocolos de sincronização de tempo de transmissão. Eles conduzem uma avaliação abrangente dos esquemas de autenticação existentes para determinar sua adequação para proteger a sincronização de tempo de transmissão. Os autores descobriram que muitos esquemas, incluindo o TESLA, não são adequados devido à vulnerabilidade a ataques de atraso de mensagens. No entanto, eles identificam duas classes promissoras de esquemas de autenticação: a classe de propagação de assinatura com o esquema RLH e a classe de assimetria híbrida com TV-HORS. Esses esquemas oferecem potencial para garantir a sincronização do tempo de transmissão, especialmente com melhorias futuras. Os autores enfatizam a importância de sua avaliação para inspirar novas pesquisas para aumentar a segurança da sincronização de tempo de transmissão, que é crucial para infraestruturas críticas, como telecomunicações, automação industrial, aviônica e distribuição de energia.

Um estudo de O'Donoghue et al. (2017) [27], analisa as preocupações de segurança em evolução na comunidade do protocolo de sincronização de tempo de rede. Seu objetivo é fornecer uma visão geral das duas soluções, o IEEE 1588 Precision Time Protocol (PTP) e o IETF Network Time Protocol (NTP), que estão sendo desenvolvidos para aumentar a segurança. Eles enfatizam a importância da segurança na sincronização de tempo, particularmente em aplicações de infraestrutura crítica. O artigo discute vários casos de uso e cenários de implantação, destacando a necessidade de soluções de segurança estáveis em transmissão de energia, automação de subestações, controle de movimento, sistemas distribuídos, sistemas de negociação do setor financeiro, institutos

de metrologia e gerenciamento de segurança. Os autores expressam otimismo de que os esforços em andamento resultarão em soluções de segurança estáveis para NTP e PTP, com coordenação entre os comitês e grupos relevantes. Eles enfatizam a importância da implementação, testes de interoperabilidade, pesquisa de vulnerabilidade e testes operacionais para garantir a robustez e a segurança das soluções propostas. Apesar do trabalho restante, um progresso significativo foi feito para o avanço das soluções de segurança para protocolos de sincronização de tempo de rede.

Uma tese de Kyriakakis (2021) [28], concentra-se em abordar os desafios da execução de tarefas com previsão de tempo e da latência de comunicação de ponta a ponta limitada em sistemas cibe físicos distribuídos. O estudo explora soluções de *software* e *hardware* para alcançar sincronização de relógio precisa e tolerante a falhas, latência mínima e execução de tarefas síncronas. O IEEE 1588 Precise Time Protocol é utilizado para sincronização de tempo, com o desenvolvimento de uma unidade de *hardware* capaz de atingir precisão de nanossegundos. O projeto tolerante a falhas proposto é avaliado e comprovadamente eficaz contra falhas e ataques de rede. Além disso, o protocolo de comunicação acionado por tempo TTEthernet é analisado e uma pilha de rede analisável por tempo é apresentada para permitir a sincronização de tarefas em tempo real. Um *framework* de código aberto é introduzido para agendar e executar tarefas distribuídas, apresentando latência e oscilação mínimas. A eficácia do *framework* é demonstrada através de sua aplicação bem-sucedida a um aplicativo de *benchmark* aviônico, executando um cenário de voo usando um *framework* acionado pelo tempo. A pesquisa mostra que as soluções propostas podem distribuir aplicações de controle em malha fechada e alcançar previsibilidade de tempo em sistemas distribuídos. As metas de validação, incluindo sincronização precisa e *jitter* mínimo de tarefas dentro de 10µs, são cumpridas com sucesso pela estrutura proposta. Uma boa abordagem foi mostrada, mas o impacto no *hardware* e na rede legada são significativos para a aplicação no tema desse trabalho.

A publicação de Itkin e Wool (2020) [29] realizou uma análise abrangente do padrão Precision Time Protocol (PTP), com foco em suas propriedades de segurança e na necessidade de medidas de segurança adicionais. Eles identificaram novos ataques e

propuseram defesas não criptográficas baseadas em rede para mitigá-los. Especificamente, eles sugeriram substituir a criptografia simétrica do Anexo K por assinaturas eficientes de chave pública de curva elíptica. Os autores implementaram e avaliaram tanto os ataques quanto as defesas propostas, demonstrando sua eficácia e praticidade em computadores padrão de prateleira. Eles concluíram que o protocolo modificado, incorporando suas contramedidas de segurança, aumenta a segurança e a robustez do padrão IEEE 1588, tornando-o uma solução de rede mais segura. O estudo também pediu que pesquisas futuras se concentrem em inspecionar formalmente a segurança do protocolo. Em geral, os esquemas propostos foram considerados altamente práticos e mais seguros do que as sugestões anteriores, oferecendo melhor proteção para redes de TI com uma demanda por relógios precisos e sincronizados, especialmente em aplicações de medição, controle e financeiras.

Annessi et. Al (2018) [30], analisou os aspectos de segurança dos protocolos de sincronização de relógio de alta precisão, particularmente sua vulnerabilidade com relação a ataques de *delay*, mesmo quando criptografados. O estudo concentrou-se no Protocolo de Tempo de Precisão (PTP) e investigou ataques de *delay* seletivo de mensagens por meio de análise estatística de tráfego. Contramedidas como ofuscação de tráfego e proteção contra repetição foram propostas para mitigar esses ataques. Os autores também introduziram ataques de *delay* de link assimétrico e argumentaram que protocolos de sincronização de relógio de alta precisão não podem impedi-los totalmente devido ao mecanismo de compensação necessário para a precisão. O artigo conclui que alcançar precisão e segurança contra-ataques de *delay* é um desafio, contradizendo a crença de que a criptografia e a autenticação podem fornecer ambas. Os ataques de *delay* representam uma ameaça à sincronização de relógio de alta precisão, limitando sua precisão, apesar da capacidade de limitar seu impacto. A precisão alcançável é mais rigorosa do que se supõe em aplicações de infraestrutura crítica que dependem de sincronização de tempo precisa, introduzindo um novo vetor de ataque.

O artigo de Kakade et al. (2022) [31], investiga as vulnerabilidades da sincronização de tempo de rede Ethernet automotiva, empregando uma simulação OMNet++. Central para sua pesquisa é um modelo de simulação gPTP projetado para

replicar uma gama de modos de falha que ameaçam a sincronização de rede. O sistema em análise é uma rede Ethernet automotiva, especificamente para quatro ECUs, cada uma comandando um dos quatro motores DC de um veículo elétrico. Os autores utilizam uma simulação OMNet++, complementada pela biblioteca INET 4.4, para modelar a topologia da rede, o protocolo gPTP e o *clock drift*. Sua análise aprofundada sob cenários de operação normal, *failover* de *clock* e ataque de *black hole* revelam a precisão de sincronização da rede de aproximadamente ±100ns e sua suscetibilidade a vários modos de falha. Eles defendem a ampliação da segurança e robustez da rede, além da implementação de verificações de redundância em cada nó da ECU.

Em um estudo digno de nota, Kim et al. (2020) [32] desenvolveu e examinou um método de sincronização de tempo para redes heterogêneas em veículos autônomos. A pesquisa estende o padrão IEEE 1588 (PTP) para redes compostas por sub-redes CAN e Ethernet conectadas por um *gateway*. Eles ainda inovaram um mecanismo PTP adequado para redes CAN e propuseram equações para calcular o atraso de propagação e compensação, considerando o tempo de processamento assimétrico no *gateway*. Uma abordagem de sincronização distinta explorando a topologia de barramento do CAN também foi proposta. Sua avaliação, por meio de um banco de testes de módulos de microcontroladores automotivos, revelou um erro de sincronização de aproximadamente 7 microssegundos entre nós CAN e Ethernet conectados ao *gateway*, indicando potencial para sincronização precisa em veículos autônomos e outras redes heterogêneas. Este trabalho amplia a base de conhecimento sobre sincronização de tempo em redes heterogêneas.

DeCusatis et al. (2020) [33] aprofundou-se nas vulnerabilidades de segurança inerentes ao padrão IEEE 1588, ou ao Precision Time Protocol (PTP), um protocolo crucial para sincronização de relógio de alta precisão em uma infinidade de aplicativos, incluindo transações financeiras em escala empresarial. Utilizando um *testbed* PTP experimental, o estudo executa e analisa com sucesso ataques que interrompem a sincronização PTP, como *spoofing* de sincronização e falsificação de *clock* mestre, examinando seus potenciais impactos e contramedidas. O estudo enfatiza a facilidade de tais ataques de ameaças internas e suas consequências potencialmente devastadoras nos sistemas

associados. Os pesquisadores propõem técnicas de mitigação envolvendo autenticação baseada em identidade ou modificações no padrão PTP. Eles ressaltam a vulnerabilidade do protocolo PTP, crucial para aplicativos sensíveis à latência, a ataques cibernéticos que interrompem a sincronização entre dispositivos PTP ou relógio do sistema e *hardware* PTP. Eles sugerem ainda que pesquisas futuras devem se concentrar em outras ameaças potenciais às redes PTP, incluindo ameaças externas e ataques originados dentro da mesma rede PTP. Este artigo fornece evidências experimentais vitais sobre vulnerabilidades de segurança PTP e soluções potenciais, melhorando nossa compreensão da ligação entre mecanismos de segurança e sincronização de temporização, um desafio significativo na criação de redes de temporização seguras e confiáveis. Esta pesquisa também introduz novos cenários de ataque e contramedidas, enriquecendo a literatura existente sobre segurança PTP.

Em seu estudo, Langer et al. (2018) [34] realiza uma análise comparativa do desempenho de sincronização de tempo entre o protocolo NTP (Network Time Protocol) padrão e o NTP protegido usando o protocolo NTS (Network Time Security). Os autores empregaram o *software* NTS da *Ostfalia University of Applied Sciences* para suas medições. Este *software* representa a primeira implementação NTS baseada no rascunho de internet da IETF "draft-ietf-ntp-using-nts-for-ntp-06". O estudo visa avaliar o impacto das medidas de segurança do NTS no desempenho da sincronização de tempo. Ao quantificar esse impacto, os autores tiram conclusões perspicazes sobre a eficiência do NTS, identificando áreas potenciais para aprimoramentos de protocolos. Em essência, seu trabalho oferece uma avaliação detalhada do desempenho de sincronização de tempo entre NTP padrão e NTS, lançando luz sobre a eficiência das medidas de segurança e fornecendo orientação para melhorias adicionais no protocolo.

No seu recente trabalho, Langer et al. (2020) [35] focou em examinar tempos de execução de *software* no contexto de implementações de protocolo de tempo de rede (NTP) e seus efeitos na sincronização de tempo. Eles propuseram várias abordagens de compensação para mitigar esses efeitos e melhorar a sincronicidade. Os resultados mostraram melhorias significativas na sincronicidade, reduzindo os desvios em uma rede local de até 85µs para quase zero, independentemente do método de compensação

utilizado. Os métodos introduzidos, como a correção direta de *timestamp* no lado do servidor ou a utilização de um campo de extensão NTP com valores medianos, ofereciam a vantagem dos servidores sem monitoração de estado. O cliente poderia compensar sua parte salvando o *timestamp* do soquete e usando-o para cálculos de deslocamento. No entanto, a obtenção de sincronicidade perfeita exigiu o suporte e a utilização de *timestamp* de *hardware* pelo cliente e pelo servidor para eliminar as latências do *software*. O estudo também enfatizou a importância de métodos compensatórios, especialmente ao usar NTS seguro NTP, pois os *timestamp*s precisam ser empacotados antes das operações criptográficas. Em geral, os resultados destacaram a eficácia das abordagens de compensação propostas e tornaram irrelevantes os argumentos contra o uso do NTS, demonstrando uma compensação fácil por qualquer degradação de compensação causada pela proteção do NTS.

A recente publicação de Langer et al. (2021) [36], propôs uma extensão para o protocolo NTS (Network Time Security), visando preencher a lacuna de comunicação entre o servidor de estabelecimento de chaves NTS (NTS-KE) e os servidores de tempo conectados. Essa extensão resolve uma lacuna de especificação descrita na RFC 8915, garantindo uma comunicação segura e independente de implementação para o protocolo NTP (Network Time Protocol) e o PTP (Precision Time Protocol). O protocolo de registro de servidor de tempo NTS introduzido complementa a especificação NTS existente, seguindo a estrutura definida no rascunho NTS4PTP. Ao combinar esta solução com NTS4NTP (RFC 8915) e NTS4PTP, um *framework* abrangente e totalmente seguro para NTP e PTP, baseada em NTS, é alcançado.

Tripathi et al. (2020) [37] apresentam um novo ataque ao protocolo NTP (Network Time Protocol) usado para sincronização de relógio. O ataque visa especificamente o modo de transmissão do NTP, impedindo que os clientes sincronizem seus relógios com o servidor. Os autores demonstram a eficácia do ataque por meio de experimentos reais de rede, destacando seu impacto nos modos de *transmissão/multicast* autenticado e não autenticado. Sua extensa varredura do espaço de endereço IPv4 revela que vários *hosts* de baixo estrato altamente precisos são suscetíveis ao ataque. O artigo propõe contramedidas para mitigar o ataque e discute os esforços em andamento para

desenvolver abordagens de prevenção eficazes. Os autores incentivam a avaliação adicional, a identificação de vulnerabilidades e a implementação de *patches* e mecanismos de defesa.

O artigo de Mkacher et al. (2018) [38] introduz o protocolo STS (Secure Time Synchronization) como uma solução para resolver falhas de segurança no protocolo NTP (Network Time Protocol). O protocolo STS permite a autenticação mútua entre clientes e servidores, oferece suporte ao não repúdio e utiliza um Servidor de Autorização (AS) para negociação e autorização. Os autores propõem um método de sincronização de tempo de inicialização para lidar com o desafio da validação de certificado que depende do tempo. Eles analisam as propriedades de segurança do STS usando a ferramenta ProVerif e implementam o protocolo estendendo o OpenNTPD. Por meio de experimentos de medição, eles avaliam o *overhead* de primitivas criptográficas para geração de código de autenticação e assinaturas digitais e comparam a precisão do STS com o NTP não autenticado. Os resultados demonstram que as primitivas escolhidas introduzem um *overhead* mínimo, e STS atinge um nível de precisão, segurança e confiabilidade comparável ao NTP.

Na pesquisa realizada por Malhotra e Goldberg (2016) [39], o foco é colocado no Network Time Protocol (NTP), descobrindo várias vulnerabilidades em seu modo de transmissão autenticado criptograficamente. Os autores demonstram com sucesso duas formas diferentes de ataques: em primeiro lugar, um ataque de repetição, permitindo que um invasor no caminho conecte indefinidamente um cliente de transmissão a um determinado horário e, em segundo lugar, um ataque de negação de serviço (DoS) que inibe o cliente de transmissão de atualizar seu relógio do sistema despachando pacotes de transmissão mal-intencionados. Os autores destacam ainda a prevalência da transmissão do NTP juntamente com outros modos efêmeros/preemptíveis por meio de medições de rede abrangentes. Essas descobertas fornecem uma compreensão mais clara das limitações dentro da atual implementação de autenticação criptográfica de chave simétrica do NTP no modo *broadcast*. Isso acaba levando os autores a sugerir medidas para aumentar a segurança geral do PNT nessas circunstâncias.

A pesquisa realizada por Aanchal Malhotra et al. (2016) [40], examina as vulnerabilidades vinculadas ao tráfego NTP (Network Time Protocol) não autenticado e as maneiras pelas quais os invasores de rede podem explorá-las para manipular o tempo dos sistemas clientes. Seu estudo explora inicialmente como um invasor no caminho, ao sequestrar o tráfego para um servidor NTP, pode facilmente manipular o tempo nos clientes desse servidor. Posteriormente, os autores introduzem um ataque de negação de serviço de pacote único que um invasor fora do caminho poderia implantar de qualquer local na rede para interromper a sincronização de relógio NTP em um cliente. Além disso, eles mostram como um invasor fora do caminho pode aproveitar a fragmentação de pacotes IPv4 para alterar drasticamente o tempo em um cliente. O artigo também discute as repercussões desses ataques em outros protocolos centrais da Internet e quantifica a superfície do ataque por meio de extensas medições da Internet. Os autores propõem várias contramedidas diretas que poderiam reforçar a segurança do NTP. Em resumo, sua pesquisa ilumina os riscos ligados ao tráfego NTP não autenticado e fornece insights para mitigar essas vulnerabilidades.

O estudo de Benjamin Dowling et al. (2016) [41] investiga a necessidade urgente de sincronização de tempo segura no Network Time Protocol (NTP), um protocolo utilizado por dispositivos conectados à rede para sincronizar seu tempo com servidores remotos. Os autores destacam que muitos serviços implementam NTP sem autenticação, e os mecanismos de autenticação existentes carecem de análise formal ou possuem fraquezas criptográficas. Para superar essas deficiências, os autores propõem uma variante autenticada do NTP, denominada ANTP. A ANTP foi projetada para proteger contra-ataques de dessincronização e, ao mesmo tempo, minimizar as operações de chave pública do lado do servidor. Esse objetivo é alcançado realizando intermitentemente uma troca de chaves via criptografia de chave pública e recorrendo à criptografia simétrica para solicitações de sincronização de tempo futuro. Notadamente, a ANTP garante que o processo de autenticação não colide com a precisão da sincronização de tempo. Os resultados indicam que a utilização de criptografia simétrica pela ANTP reduz a taxa de transferência do servidor para solicitações de sincronização de tempo em apenas um fator de 1,6 em comparação com o NTP convencional. Em essência,

o estudo introduz a ANTP como uma iteração autenticada do NTP, abordando o requisito de sincronização de tempo segura, garantindo segurança aprimorada e mantendo um desempenho razoável.

Em sua pesquisa, Langer et al. (2019) [42] concentram-se na necessidade essencial de sincronização de tempo segura dentro do protocolo NTP (Network Time Protocol). Eles introduzem uma variante autenticada, ANTP, projetada para evitar ataques de dessincronização e minimizar as operações de chave pública do lado do servidor. A eficácia do ANTP é avaliada no OpenNTPD usando OpenSSL, demonstrando que sua implementação de criptografia simétrica afeta apenas ligeiramente a taxa de transferência do servidor para solicitações de sincronização de tempo. A segurança da ANTP também é analisada sob uma nova estrutura de segurança demonstrável, ilustrando sua capacidade de alcançar sincronização de tempo segura. O estudo estabelece a ANTP como uma solução robusta que equilibra segurança aprimorada com eficiência de desempenho.

Em seu trabalho, Aanchal Malhotra et al. (2017) [43] aprofundam-se nos meandros de segurança do protocolo de datagrama NTP (Network Time Protocol), essencial para sincronizar relógios de computador em rotas de rede inseguras. Os autores criticam que o protocolo de datagrama NTP, conforme delineado na RFC5905, é inadequadamente definido e intrinsecamente falho. Eles destacam três questões principais: consideração insuficiente das necessidades de segurança díspares em diferentes modos NTP, ineficácia do mecanismo de combate a ataques fora do caminho e a exposição de informações confidenciais por meio da interface de consulta de controle do NTP que poderiam ser potencialmente exploradas. Eles apresentam várias estratégias de ataque que um adversário remoto poderia utilizar para manipular maliciosamente o tempo em um sistema alvo. Suas varreduras de rede revelam milhões de IPs vulneráveis. Para mitigar essas falhas de segurança, os autores apresentaram um modelo criptográfico, demonstrando sua segurança enquanto propunham um novo protocolo cliente/servidor compatível com versões anteriores para NTP.

Outras Propostas

Teichel et. al (2018) [44] propõe o uso de mecanismos secundários de *watchdog* para proteger os protocolos primários de sincronização de tempo contra erros. Eles se concentram em cenários em que o mecanismo *watchdog* fornece proteção criptográfica mais forte do que o mecanismo de sincronização primário, que emprega comunicação unidirecional com divulgação atrasada de informações criptográficas. Os autores apresentam resultados experimentais da combinação do mecanismo primário com um mecanismo de controle bidirecional seguro e recomendam essa abordagem. Eles enfatizam os benefícios da combinação de vários protocolos de sincronização, com um protocolo unidirecional como o primário e um protocolo bidirecional como o *watchdog*. Embora reconheçam o aumento da complexidade, eles destacam as vantagens dessa abordagem e sugerem trabalhos futuros sobre provas formais de propriedades de segurança, melhorando o mecanismo *Guard*, acomodando protocolos primários específicos e explorando máquinas com reconhecimento de origem e de canal. Em geral, os autores visam aumentar a segurança de sistemas de sincronização de tempo de alta precisão.

No artigo de Zheng et al., (2021) [45], o objetivo é propor uma nova estratégia de segurança baseada na codificação polar para sincronização de tempo de rede, abordando questões relacionadas a ataques de *delay* e adulteração de *timestamp*. O sistema de destino inclui qualquer abordagem de tempo seguro que possa ser suscetível a tais ataques. Os autores realizam análises teóricas e propõem sua estratégia de segurança, seguida de simulações para medir seu desempenho. A abordagem proposta utiliza polarização de canal para estabelecer canais de bits seguros para troca de *timestamp* e detecção de pacotes de sincronização atrasados. Operar na camada física garante a compatibilidade com os protocolos de segurança existentes, alcançando a segurança da transmissão sem criptografia. Os resultados da simulação confirmam a eficácia da estratégia, enfatizando suas vantagens como retro compatibilidade, baixa complexidade computacional e baixo atraso de processamento. O documento oferece insights valiosos para o aprimoramento dos protocolos de segurança de sincronização de tempo de rede.

2.2 - Discussão

O gerenciamento de chaves criptográficas em ambientes embarcados em veículos é uma área de pesquisa em rápido desenvolvimento. A análise de artigos, teses, literatura cinzenta e outras normas permitiu definir o seguinte estado da arte:

Seguindo os passos utilizados durante a revisão, vimos que a definição de uma arquitetura segura e a criação de uma relação de confiança entre as entidades por meio de material criptográfico, fruto de um sistema de gestão de chaves eficaz, são desafios encontrados não apenas no ambiente automotivo, mas também em outros ambientes como *Smart Grid* e Internet das Coisas. Muito trabalho foi feito e é possível observar a relevância do tema crescendo e as muitas tentativas de reutilizar as melhores práticas disponíveis, mas não existe uma solução de prateleira que possa ser utilizada sem algum tipo de customização.

Quanto a como garantir uma fonte de comunicação *off-board* com o veículo, a fim de equipá-lo com uma fonte confiável de tempo, muitos estudos foram feitos, com resultados promissores. Além dos protocolos propostos, novos e reutilizados, as normas já definem uma forma de transmitir essas informações. No entanto, o grande problema é a interoperabilidade do uso do GNSS em todo o mundo. Por enquanto, temos apenas soluções regionalizadas, como a proposta pelo NIST, o que dificulta sua aplicação quando se trata de uma solução que funciona em várias partes do mundo, como é necessário no mercado automotivo.

Passando para o compartilhamento de informações de tempo de forma segura através da rede veicular embarcada, vimos que mecanismos e protocolos consolidados como TESLA, PTP e NTP, além dos problemas de segurança ainda não totalmente mitigados, enfrentam problemas de aplicação em ambientes automotivos, ou similares, em termos de *hardware* necessário em cada nó para gerenciamento de tempo do lado do cliente, bem como a limitação de soluções para aplicação em redes híbridas como as encontradas atualmente em arquiteturas eletrônicas veiculares, com rede ethernet, CAN, FlexRay, LIN e etc.

Assim, a partir do claro entendimento do estado da arte, do que já foi executado, do que funcionou e do que ainda requer uma continuidade dos trabalhos, encerramos a revisão bibliográfica com a clara definição das lacunas atuais em relação ao sistema automotivo:

1 - Uma arquitetura de link criptográfico entre o veículo e um servidor confiável que tem interoperabilidade mundial.

2 - Uma arquitetura de link criptográfico intra-veicular que permite o compartilhamento seguro entre ECUs de informações de tempo.

3 - Um protocolo de compartilhamento de tempo que é agnóstico em termos de topologia de rede, *payload* com tamanho compatível com as limitações de redes legadas, como a CAN, e proteção contra manipulação de conteúdo de mensagem.

Capítulo 3
Metodologia

Para a realização do projeto e consequente dissertação, optou-se pela metodologia DSR (Design Science Research). Para evitar uma desvinculação do trabalho realizado com a relevância do tema para a área pesquisada, a escolha da metodologia correta é fundamental. Como a pesquisa e a dissertação buscam sua aplicação nas áreas de tecnologia e engenharia, o método DSR auxilia durante o desenvolvimento das atividades a avaliação contínua da relevância do tema e sua aplicabilidade no mundo real conforme descrito por Vaishnavi e Kuechler (2004) [46].

Para entender a metodologia e sua aplicação, duas terminologias são de entendimento essencial, conceito e artefato. Conceito é uma ciência que busca consolidar o conhecimento sobre o projeto e desenvolvimento de soluções para melhorar sistemas existentes, resolver problemas e criar artefatos. Artefato é um construto, modelo, método ou instanciação construído pelo pesquisador. Interface entre o ambiente interno e o ambiente externo de um determinado sistema.

É importante que as soluções apresentadas sejam satisfatórias. Serão soluções suficientemente adequadas ao contexto em questão. Devem ser viáveis, não necessariamente grandes. Verificar a área de pesquisa proposta se mostra fundamental, pois não adianta apresentar uma solução ótima, mas não aplicada às limitações de sistemas embarcados, como os automóveis. Também é preciso que haja uma validade pragmática. Durante o processo é necessário garantir a utilidade da solução. Um ponto importante é o custo/benefício da solução, particularidades do ambiente em que será aplicada e as reais necessidades dos interessados na solução. Novamente, no ambiente estudado, o custo para sua utilização poderia ser inviável.

Outro ponto relevante da metodologia para o projeto proposto é o conceito de classes de problemas. Isso orienta a organização da trajetória e o desenvolvimento do conhecimento no âmbito da ciência do design. Sistemas embarcados em automóveis se assemelham a sistemas embarcados em aviões, embarcações, máquinas agrícolas e outros dispositivos IoT. Dessa forma, durante a trajetória trabalhar com essas classes de problemas ajudará que, mesmo que a solução esteja focada em um mercado específico,

seus resultados também podem ser aplicados em outros mercados que se enquadram na mesma classe de problemas.

Ao contrário da ciência natural ou da ciência social, a ciência do design ajuda a focar o propósito em projetar, produzir sistemas que não existem ou modificar situações existentes para alcançar melhores resultados. Mantem o foco na solução, que é extremamente relevante para o projeto proposto. O objetivo da pesquisa dentro da Design Science é prescrever, orientar a pesquisa para a solução de problemas específicos. Isso nos ajuda a orientar as atividades para a solução do problema proposto e não nos perdermos em explorar ou descrever o problema como outras metodologias fariam.

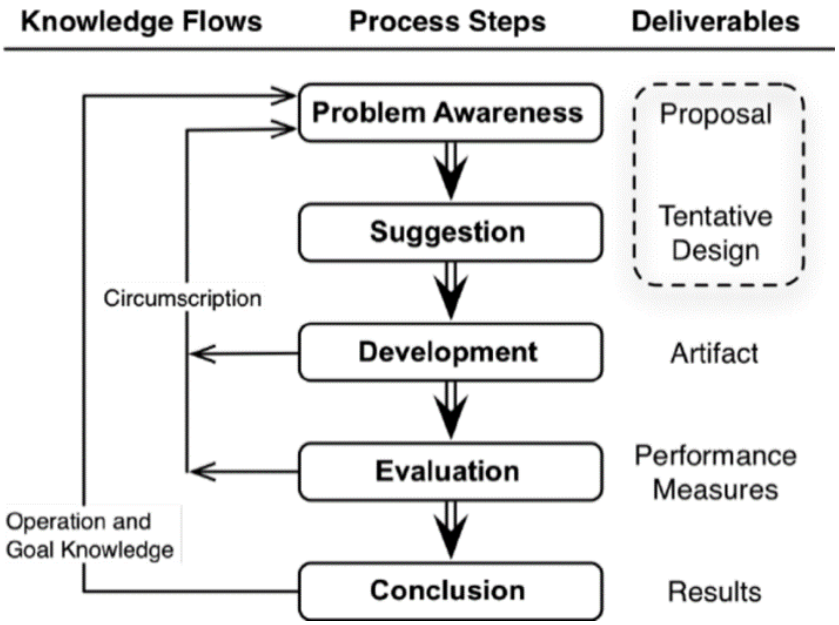


Figura 4 - Design Science Research (Vaishnavi & Kuechler, 2004)

Na Figura 4 vemos a descrição das etapas propostas pela metodologia e como deveríamos segui-las durante o desenvolvimento do projeto. A dissertação deveria ser estruturada seguindo os passos da metodologia. As diretrizes metodológicas devem ser a espinha dorsal da pesquisa, estando presentes em cada capítulo. Temos a obrigação na primeira diretriz de construir um artefato, que se alinhe com o modelo que resolve o problema especificado e irá gerar o necessário para a definição do referencial teórico da dissertação. Assim, objetivamos construir um artefato na forma de um aplicativo de *software*, rodando em um ambiente de aplicação real (uma unidade eletrônica

automotiva), de onde podemos extrair as informações necessárias para avaliação da solução.

3.1 - Como a Design Science Research foi utilizada nesse trabalho

Como descrito anteriormente, este estudo seguiu as diretrizes do DSR durante cada fase da pesquisa para garantir o fluxo correto das atividades e o rigor das realizações durante o desenvolvimento da solução. A segunda diretriz do DSR traz a relevância do problema, que será definida pelas etapas de identificação, conscientização, revisão da literatura e identificação dos artefatos a serem desenvolvidos que atendam a uma classe de problemas. Tudo isso gerará a base para a contextualização do problema, definindo a descrição do problema e a revisão da literatura na dissertação. Foi a estrela norte do capítulo "Problemas e Objetivos" por uma clara identificação e definição do problema. Isso foi possível por meio de uma revisão sistemática da literatura captada pelo capítulo "Referencial Teórico" que a partir de sua última seção, *Discussão*, traz o estado da arte do campo em pesquisa e deixa claro quais são os problemas ainda em aberto nesse campo.

Durante o desenvolvimento da solução proposta descrita no capítulo "Proposta de Artefato", sempre esteve presente a primeira diretriz de DSR sobre a definição e criação de um artefato que permitisse validar o modelo, orientando o que deveria ser implementado para extrair a avaliação necessária da solução. Além disso, a sexta diretriz foi importante para garantir um desenho de uma solução que pudesse ser feito como um processo de pesquisa. A possibilidade de amadurecer o artefato à partir das interações permitiu que definições teóricas, como o tamanho dos quadros do protocolo, pudessem ser refinadas para o tamanho adequado após a devida implementação e avaliação do protótipo.

A terceira diretriz DSR garante que o método de avaliação utilizado é eficaz. Esteve presente em cada passo seguido desde a introdução até a conclusão. Durante a definição do problema e revisão da literatura, foi perguntado como poderíamos ter certeza de que o problema identificado tinha uma maneira clara de ser verificado em torno da eficácia de uma possível solução compatível. Durante o capítulo "Demonstração, Avaliação e

Conclusões", fica ainda mais claro onde foram considerados todos os aspectos relevantes em torno da resiliência de segurança cibernética da solução.

É importante ressaltar que, como trabalho científico, o rigor necessário da pesquisa deve estar sempre em presente. Foi demonstrada a utilização de ferramentas automotivas profissionais, e a mentalidade do design como um processo de pesquisa, seguindo a quinta e sexta diretrizes, para garantir o bom desenvolvimento do projeto e seu registro na dissertação. Como mostrado durante a sessão *Implementação*, foram utilizadas ferramentas consolidadas no mercado de engenharia de *software* para o desenvolvimento e validação do artefato e seu armazenamento.

A quarta diretriz reforça a contribuição da pesquisa para a área de aplicação. Durante o desenvolvimento da solução apresentada, foi realizada uma constante reavaliação do custo/benefício da solução, sua aplicabilidade frente às limitações do sistema embarcado. O objetivo foi trazer contribuição científica sem perder a possibilidade de implementar a solução em um sistema automotivo real. Finalmente, a sétima diretriz que sustenta a definição da comunicação de resultados utilizando meios apropriados constitui a base para a condução das conclusões do projeto, sua aplicação a uma classe de problemas e a comunicação dos resultados apresentados neste documento.

Capítulo 4
Problemas e Objetivos

4.1 - Identificação e Conscientização do Problema

Como descrito na introdução, o problema identificado é ao usar material criptográfico dentro de sistemas automotivos para validar uma mensagem, ou autenticar um usuário, é necessário ter uma fonte confiável de tempo para que uma chave ou certificado expirado não seja usado incorretamente. No entanto, soluções prontas para uso comuns em sistemas de TI não funcionam para sistemas automotivos embarcados. Vimos anteriormente que estamos lidando com um ambiente razoavelmente limitado em termos de *hardware*, seja de processamento ou seja a presença de dispositivos para gerar e manter informações de tempo, como RTCs. Além disso, as redes de comunicação entre os módulos veiculares possuem limitação de largura de banda, muitas vezes lidando com a arbitragem de mensagens de prioridade de colisão, como no caso da rede CAN conforme descrito na ISO 11898-1:2015 [47].

Temos vários casos de uso presentes hoje no setor automotivo que exigem a validação de certificados por ECUs que antes não tinham preocupação com a questão da segurança. Podemos citar um possível controle de acesso para a realização do diagnóstico, reparo e atualização de *software*, seja físico ou remoto, com diferentes níveis de autorização. Temos ainda novos sistemas de carregamento de veículos elétricos com autorização de pagamento via linha de energia. Até mesmo a ativação de pacotes de funções através de assinatura mensal, que podem expirar ou ser canceladas pelo usuário, são agora realidade.

Voltando aos métodos científicos onde a metodologia está ancorada, precisamos ampliar a compreensão do problema então identificado. Segundo Kitchenham, B. (2004) [48], do tema traçado surgem questões relevantes e fundamentais no processo de construção da pesquisa:

1 – Se a gestão de chaves de criptografia, e consequentemente as informações de tempo necessárias para sua correta execução, já é um tema bem trabalhado na área de segurança da informação, por que a dificuldade de sua aplicação em sistemas veiculares?

2 – Quais as limitações do sistema embarcado em veículos que impedem a aplicação de uma solução de gerenciamento de *timestamp* para chaves criptográficas já maduras no universo convencional da informática?

3 – Há outros campos de pesquisa com limitações semelhantes nos quais poderíamos reutilizar os resultados encontrados, como o recente campo da Internet das Coisas, sua ampla exploração e suas semelhanças?

Kitchenham também introduz a importância dos métodos. Quais são os exemplos de observação? Quais métricas são necessárias para assumir que uma solução seria ideal para o sistema e suas limitações? Existem modelos ou *frameworks* que podem ser reaplicados (como IoT)? Quais métodos de pesquisa têm as referências na área utilizadas?

Essas e outras questões foram respondidas durante *a* sessão de discussão, como principal produto da revisão sistemática da literatura e servirá de base para a pesquisa proposta.

4.2 - Objetivos da Pesquisa

Esta seção tem como objetivo abordar as lacunas encontradas sobre o atual estado da arte, a partir da revisão sistemática da literatura realizada, destacando contribuições deste trabalho de pesquisa para esta área do conhecimento.

Em um veículo, há vários ECUs e componentes interagindo entre si, direta e indiretamente. Geralmente, uma arquitetura veicular possui pelo menos uma ECU com maior capacidade computacional e recursos de *hardware* que podem garantir maior segurança, como a presença de *trustzones*. Nosso objetivo é propor um modelo que possa usar esses poderosos ECUs para resolver as três principais lacunas identificadas a partir do estado da arte. Essas ECUs, aqui neste trabalho chamadas *Primary ECUs* (PECUs) estão genericamente ligados a outras ECUs, aqui identificadas como *Secondary ECUs* (SECU) através de módulos de *gateway*, com a capacidade de converter mensagens de uma tecnologia de rede para outra, como *ethernet* para rede CAN.

Entendendo esse tipo de topologia arquitetônica, podemos após a revisão da literatura identificar algumas classes de problemas que precisam ser resolvidos na criação de uma solução que dê a uma SECU a capacidade de usar o recurso de *timestamp* com segurança. Na Figura 5 vemos quais são essas classes identificadas:

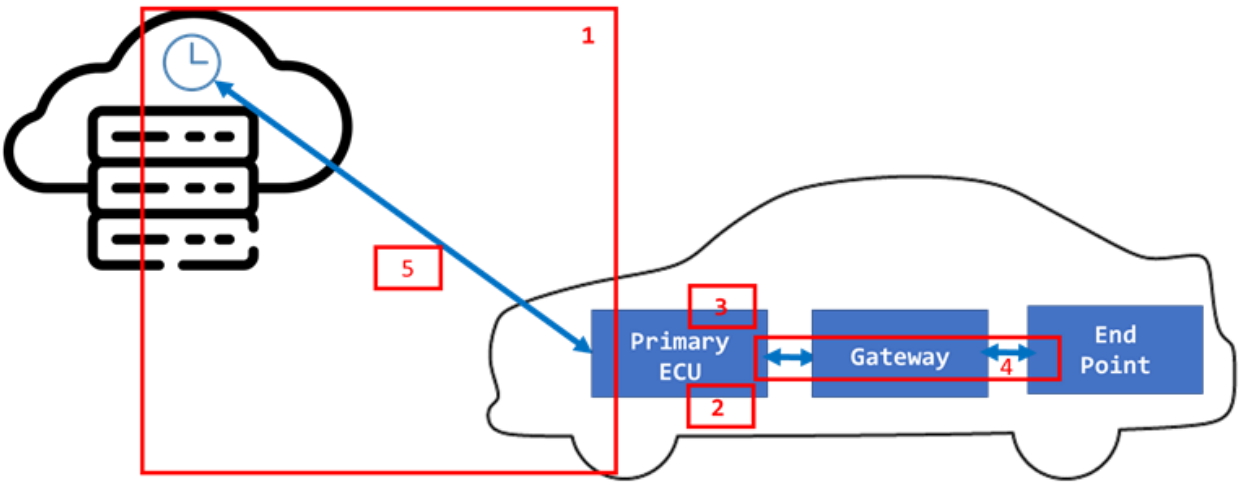


Figura 5 - Classes de problemas identificados.

1 – Classe para a conexão entre o veículo e o servidor de relógio seguro.

2 – Classe para a proteção do relógio contra manipulação.

3 – Classe para reportar a tentativa de manipulação.

4 – Classe para o compartilhamento seguro da informação de tempo entre as ECUs no veículo.

5 – Classe para os casos de uso offline (SECU sem conexão com a PECU).

Seguindo as diretrizes da metodologia DSR, este trabalho visa estreitar os problemas identificados, selecionando uma ou duas classes, tentando resolvê-los e, em seguida, investigar durante a implementação se a solução proposta pode resolver qualquer uma das outras classes de problemas.

Na figura 5, assumimos que a PECU possui dados de relógio seguros e um ambiente de *hardware* seguro para garantir a proteção das informações contra

manipulação. Além disso, partimos do pressuposto de que o veículo está conectado a um servidor autenticado, da montadora, para receber as informações de tempo. Este servidor deve ser acessado de qualquer parte do mundo através de uma conexão ad-hoc. Essa conexão será suficiente para resolver a lacuna relacionada à falta de segurança e interoperabilidade do sistema GNSS e associar soluções de segurança, que devem alimentar o carro com os dados *off-board*. Também não nos concentraremos em casos de uso off-line em que o ponto final, SECU, precisa verificar o *timestamp* sem informações provenientes do PECU. Por isso, o foco deste trabalho é resolver a classe 4, que é o compartilhamento seguro dos dados do relógio com os *end points* (SECUs) dentro do veículo.

Trazendo os aprendizados da revisão de literatura, a contribuição esperada deste trabalho é uma solução personalizada para criar uma relação de confiança entre a PECU e a SECU que permita o compartilhamento dessas informações de forma segura. Uma vez estabelecida essa relação, é necessária a proposição de um protocolo que funcione onde a aplicação de protocolos consolidados falhou em estudos anteriores. Finalmente, precisamos validar se a solução proposta é resistente a ataques cibernéticos emergentes. Como mencionado anteriormente, uma solução pronta para uso não foi encontrada e a aplicação dos mecanismos e protocolos existentes não é viável. Novamente, seguindo a metodologia DSR, a solução proposta visa trazer uma contribuição científica que possa ser utilizada por qualquer montadora que enfrente problemas semelhantes ou mesmo para outros sistemas críticos de segurança de outras áreas parecidas, como máquinas agrícolas, aviões, trens e etc.

Capítulo 5
Proposta de Artefato

5.1 - Requisitos

Após a realização de uma ampla revisão sistemática da literatura, uma lacuna significativa na pesquisa existente foi identificada, necessitando de uma solução para abordar as questões inexploradas neste estudo.

O primeiro requisito é a necessidade de uma fonte de tempo externa que possa fornecer ao *Primary Electronic Control Unit* (PECU) informações de tempo confiáveis. Quando o veículo está conectado, torna-se crucial garantir que a gestão do tempo do mestre central seja precisa, conforme salientado por Spanghero et al. (2023) [20].

Supondo que a PECU tenha implementado controles de segurança robustos de *hardware* e *software* para evitar qualquer manipulação de dados de tempo, esse aspecto não precisa ser abordado na implementação do artefato. No entanto, é importante notar que o *Secondary Electronic Control Unit* (SECU) não possui os recursos de *hardware* e *software* necessários para manter as informações de tempo de forma independente. Consequentemente, precisa contar com a PECU para solicitar e adquirir essas informações.

Portanto, o segundo requisito envolve a implementação de um protocolo leve de solicitação e resposta de tempo entre as unidades de controle, seguindo os princípios de Sherman et al. (2021) [22]. Esse protocolo deve ser projetado para abordar as limitações normalmente encontradas em redes automotivas legadas, como a rede CAN, garantindo uma comunicação eficiente.

Considerando que o protocolo requer a incorporação de autenticação criptográfica entre as unidades de controle, o terceiro requisito envolve o estabelecimento de um sistema de relação de confiança entre as centrais, conforme também trabalhado por Mahmood et al. (2018) [16]. Este sistema facilitará a troca de informações relacionadas com o tempo, garantindo simultaneamente a autenticidade e a integridade dos dados transmitidos.

Por fim, o quarto requisito enfatiza a necessidade de que as informações de tempo trocadas sejam protegidas por meio de operações criptográficas, evitando assim

qualquer adulteração não autorizada por potenciais invasores, ainda seguindo Mahmood et al. (2018) [16]. Ao empregar técnicas robustas de criptografia, o sistema deve garantir a integridade e a confidencialidade dos dados de tempo, aumentando a segurança geral das unidades de controle em rede.

5.2 - Proposição de um Modelo para Resolução do Problema

Com base nos requisitos estabelecidos, propomos um modelo abrangente para enfrentar os desafios identificados. O primeiro passo nesse modelo é o estabelecimento de uma relação de confiança entre o *Primary Electronic Control Unit* (PECU) e *o Secondary Electronic Control Unit* (SECU). Para garantir um foco na classe de problema específica e atender aos requisitos, assumimos que a PECU tem acesso a uma fonte de tempo externa segura e autenticada, juntamente com recursos robustos de gerenciamento de tempo para evitar manipulação. O escopo de nossa proposta está centrado na comunicação dentro do veículo.

Para criar a relação de confiança entre PECU e SECU, nosso modelo sugere um mecanismo de compartilhamento de chaves durante as etapas de projeto das centrais e montagem do veículo em linha. Essa abordagem leva em conta as limitações do poder de processamento e largura de banda de rede, garantindo a troca segura de chaves entre as unidades de controle.

Além disso, o modelo proposto enfatiza a necessidade de desenvolver um protocolo que possa acomodar as diversas tecnologias de rede encontradas nos veículos modernos. Este protocolo facilitará a comunicação eficiente de pedidos e respostas entre as ECUs, tendo em conta as características específicas da rede de cada veículo.

Crucialmente, o modelo prioriza a segurança e a resiliência contra-ataques de rede comuns. Ele incorpora medidas para proteger contra manipulação de conteúdo de mensagens de tempo, ataques de repetição (*replay*) e outras ameaças potenciais à integridade e autenticidade das informações de tempo.

Ao adotar este modelo, pretendemos fornecer uma solução abrangente e robusta que atenda aos requisitos identificados, garantindo uma sincronização de tempo segura e confiável entre as unidades de controle em sistemas automotivos.

5.3 - Proposta

Como mencionado anteriormente, a PECU que tem capacidade de receber tempo seguro de fonte externa autenticada, diferentemente da SECU que não possui essa capacidade, seja por limitações de conectividade ou de *hardware*.

A PECU validará o tempo recebido de fonte de tempo segura externa aplicando algum processo de validação e verificação. Este passo é uma suposição e não abordado neste trabalho. O próximo passo é que a PECU compartilhará o tempo seguro verificado com as SECUs na rede de veículos e garantirá que eles receberam o tempo autorizado.

Nessa abordagem, a SECU solicitará o tempo seguro da PECU com base na necessidade desse tempo, por exemplo, a cada ciclo de energia, a cada inicialização da SECU ou toda vez que a SECU validar as chaves ou certificados.

A PECU criará uma mensagem de tempo seguro sempre que a SECU a solicitar, o que também minimizará a carga na rede e melhorará o desempenho. Essa mensagem deve ser distribuída com segurança, incluindo integridade e autenticidade. Um dos principais pontos que essa abordagem resolve é a proteção contra-ataques conhecidos, como a proteção contra replay. Como o objetivo principal é criar uma solução para compartilhar as informações de tempo de forma segura, as seções seguintes primeiro proporão um protocolo seguro para compartilhá-las e, em seguida, apresentarão uma abordagem de gerenciamento de chaves para permitir que o protocolo seja validado usando o material criptográfico compartilhado com segurança.

5.4 - Visão Geral

5.4.1 - Formato de Tempo para a Mensagem Segura de Tempo

O formato de tempo para validação do certificado pode variar dependendo do certificado específico e dos padrões ou protocolos que estão sendo usados. Portanto, é essencial consultar os padrões ou especificações relevantes para determinar o formato de tempo exato e os campos usados para validação de certificado em um contexto específico. No entanto, um formato de hora comumente usado para validação de certificado é o formato UTC (Universal Coordinated Time). O *X509 V3 (X.509: Information technology - ITU* (2019) [49] é o formato padrão de certificado selecionado para ser usado neste projeto, pois é um formato comum usado no espaço automotivo. O formato é mostrado na figura 6.

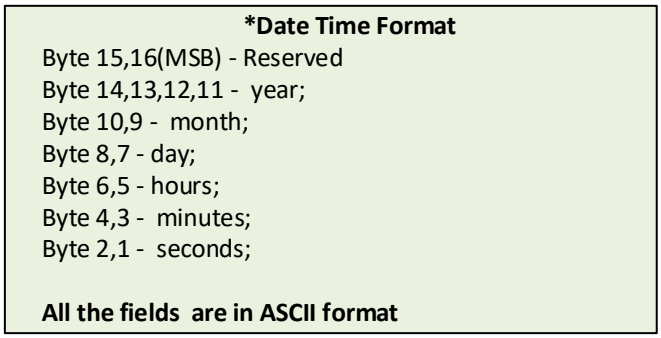


Figura 6 - Formato de Dados de Tempo

5.4.2 - Protegendo a Mensagem de Tempo

Como a mensagem de tempo está viajando entre as ECUs, há considerações de segurança que devem ser levadas em conta, como confidencialidade, integridade e autenticação, como destacado por Jason A. (2019) [50]. A confidencialidade não é exigida na mensagem de tempo seguro, mas a Integridade e a Autenticidade são necessárias para garantir a resiliência solicitada contra os ataques.

Para fornecer a Integridade e Autenticidade necessárias da mensagem de tempo, as chaves criptográficas devem ser distribuídas com segurança antes de verificar a autenticidade e a integridade da mensagem de tempo. Este projeto é baseado no Código de Autenticação de Mensagem (MAC) de chave simétrica exclusiva, onde a PECU e a SECU compartilham a mesma chave simétrica exclusiva. Ambas as entidades gerarão MAC e a sua função *hash* (HMAC), incluindo a chave simétrica exclusiva para verificar a autenticidade uma da outra. A eficácia dessa abordagem é muito bem demonstrada por muitas normas e trabalhos ao longo dos anos como Mihir et al. (1996) [51]. A PECU gerará e compartilhará com segurança a chave simétrica exclusiva com a SECU por meio de um processo de Sistema de Gerenciamento de Chaves Criptográficas (KMS).

Para outras considerações de segurança, como ataque de *replay*, a técnica de troca de *nonce* é usada para impedir que o invasor responda com qualquer mensagem de tempo utilizada anteriormente, como demonstrado por Neuman (1996) [52]. Portanto, os *nonces* são trocados com segurança usando chave simétrica única toda vez que a SECU solicita o tempo seguro da PECU. Além disso, um número exclusivo de identificação da ECU, definido anteriormente, faz parte do MAC para confirmar que a mensagem de tempo foi enviada de uma entidade autorizada.

A Figura 7 mostra a estrutura da Solicitação de Mensagem de Tempo Seguro da SECU. O quadro é então composto pelo comando *request*, número de identificação único da ECU para fornecer autenticidade, o *nonce* para fornecer proteção contra-ataque de repetição e, finalmente, o cálculo HMAC para garantir a integridade.

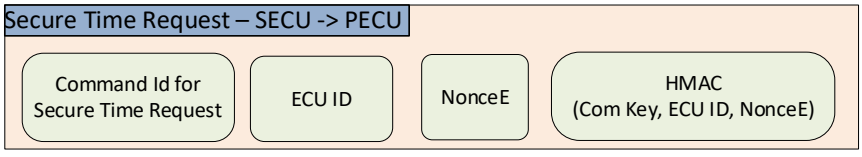


Figura 7 - Quadro de Requisição de Tempo Seguro

A PECU verificará o MAC na solicitação e responderá com a mensagem de tempo segura, conforme mostrado na figura a seguir. Um comando de status foi adicionado para

fornecer informações necessária, como qualquer falha identificada na mensagem de *request* por exemplo.

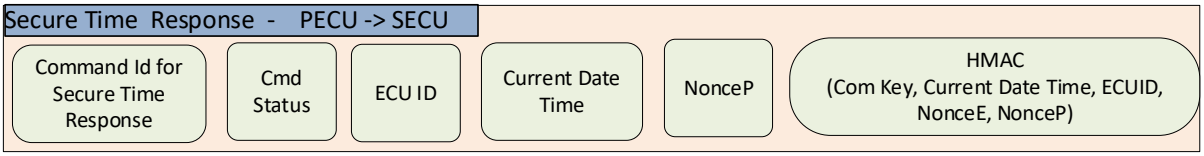


Figura 8 - Quadro de Resposta de Tempo Seguro

5.4.3 - Chave simétrica para Mensagem de Tempo Seguro

Para criar a relação de confiança entre os ECUs, é proposto um processo de gestão de chaves criptográficas. A PECU é responsável por gerar e distribuir a chave simétrica exclusiva para a mensagem de segura de tempo. Essa chave simétrica será usada para proteger a solicitação e a resposta da Mensagem de Tempo. Neste projeto, a chave simétrica utiliza a o esquema AES 128 e é chamada *Communication Key* (Com Key), conforme recomendado por Morris et al (2001) [53], uma indicação NIST viável para todos os sistemas automotivos embarcados. Antes que ambas as entidades possam usar a Com Key, a mesma deve ser distribuída de forma segura. O Secure Time conta com o sistema de distribuição de chaves conhecido como *Vehicle Key Management System* (VKMS). Durante o processo de fabricação do veículo ou ao substituir um dos ECUs, a PECU criará um vínculo de confiança com a SECU (conhecido como *trust bonding*) e, em seguida, compartilhará com segurança a Com Key. Todo o processo de chaves pré compartilhadas nos fornecedores de ECUs, bem como o processo realizado durante a montagem do veículo e em sua posterior substituição numa operação de reparo, é gerenciado pelo sistema VKMS.

Trust Bonding (TB) é um processo em que a PECU usará as credenciais pré-compartilhadas durante a fabricação das ECUs pelo fornecedor, para autorizar a SECU. Então, se a SECU for uma ECU autorizada, o processo de Trust Bonding poderá continuar

entre a PECU e a SECU. A PECU usará então a credencial de pré-compartilhamento para garantir a distribuição do Com Key, que será única por ECU.

Há várias considerações de segurança foram levadas em conta no processo de Limite de Confiança, como Autenticação, Integridade, Confidencialidade e Disponibilidade.

Distribuição da Communication Key

O processo de *Trust Bonding* é a fase em que a Com Key será distribuída entre a PECU e a SECU. O *Trust Bonding* pode ser dividido em duas fases principais:

1. Autorização da SECU

Na fase de autorização da SECU, A PECU solicitará a comprovação de autorização da SECU, solicitando a geração de MAC usando as credenciais pré-compartilhadas. A SECU enviará o comprovante de autorização a PECU. Em seguida, a PECU verificará o comprovante de autorização. Se a prova de autorização da SECU tiver sido verificada com sucesso, então a PECU irá gerar e compartilhar a Com Key com a SECU. O processo de geração de chaves com deve seguir o padrão NIST SP 800-133 (2020) [54].

2. Distribuição da chave de comunicação

Antes da distribuição da Com Key, O *Nonce* deve ser compartilhado de forma segura entre a PECU e a SECU para evitar ataques de *replay*. Em seguida, a PECU irá embrulhar a Com Key com a credencial pré-compartilhada e compartilhará encapsulado contendo a Com Key com a SECU. A técnica de envelopamento de chaves deve seguir o padrão NIST SP 800-38F (2012) [55]. Na mensagem de distribuição, a autorização e a integridade devem ser atingidas. O MAC será fornecido para garantir a integridade e autenticação. Neste projeto é utilizado o protocolo AES GCM para isso, seguindo a recomendação do padrão NIST SP800-38D (2021) [56]. Para fornecer disponibilidade, contra-ataques de negação de serviço, a PECU definirá um tempo limite (250ms) cada vez que a Com Key é distribuída para a SECU, como melhores práticas neste tipo de troca de mensagens em

uma rede de veículos. A SECU responderá com *Timeout* em caso de problemas. O quadro completo é mostrado na figura 9.

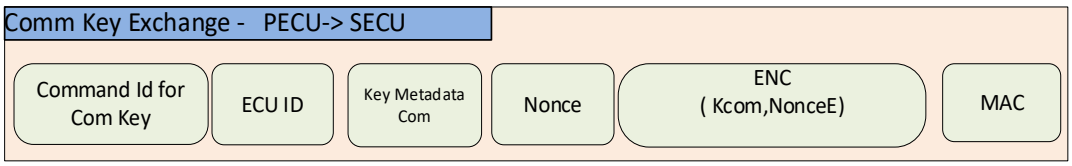


Figura 9 - Troca de chave de comunicação

A SECU deve desembrulhar e verificar a integridade da Com Key, e em seguida, confirmar o recebimento com um ACK. No caso de a SECU responder com um ACK negative (NACK), ou não responder dentro da Janela de Timeout, a PECU deve tentar novamente por duas vezes consecutivas, sempre com o *Timeout* de 250ms a cada nova tentativa. Se a PECU não receber resposta positiva ou negativa (ACK or NACK) após as 3 tentativas, então o erro deverá ser registrado na memória de erros da ECU, conhecida como DID, novamente seguindo as melhores práticas automotivas. O quadro ACK é mostrado na figura 10.

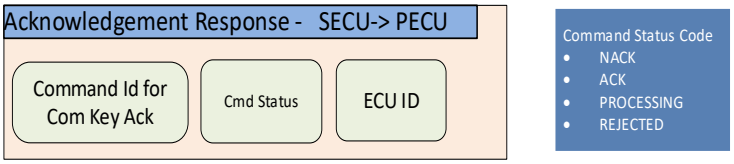


Figura 10 - Quadro de resposta para o recebimento da chave de comunicação

No caso de a PECU receber a resposta de confirmação de recebimento da Com Key da SECU, a credencial pré-compartilhada não será mais usada, e a chave Com Key será a chave utilizada para proteger a comunicação entre a PECU e a SECU, sendo única para cada veículo. A Com Key será usada também para proteger a mensagem de tempo, sendo esse um dos muitos casos de usos de comunicação segura entre as ECUs. A figura 11 mostra um diagrama que ilustra a fase de *Trust Bonding*, incluindo *handshake* de distribuição da Com Key. Vemos na figura o processo fim a fim, com os devidos fluxos de comunicação e tempo de aguardo das repostas. Conforme descrito anteriormente, as

ECUs recebem uma credencial compartilhada anteriormente durante o seu processo de produção individual. O Trust Bonding, portanto, acontece na linha de montagem do veículo, com a distribuição de chaves únicas por carro, utilizando as credenciais compartilhadas anteriormente com meio de encapsulamento seguro delas. Esse é um passo fundamental para a implementação da solução de compartilhamento seguro que seja resiliente aos ciberataques atuais.

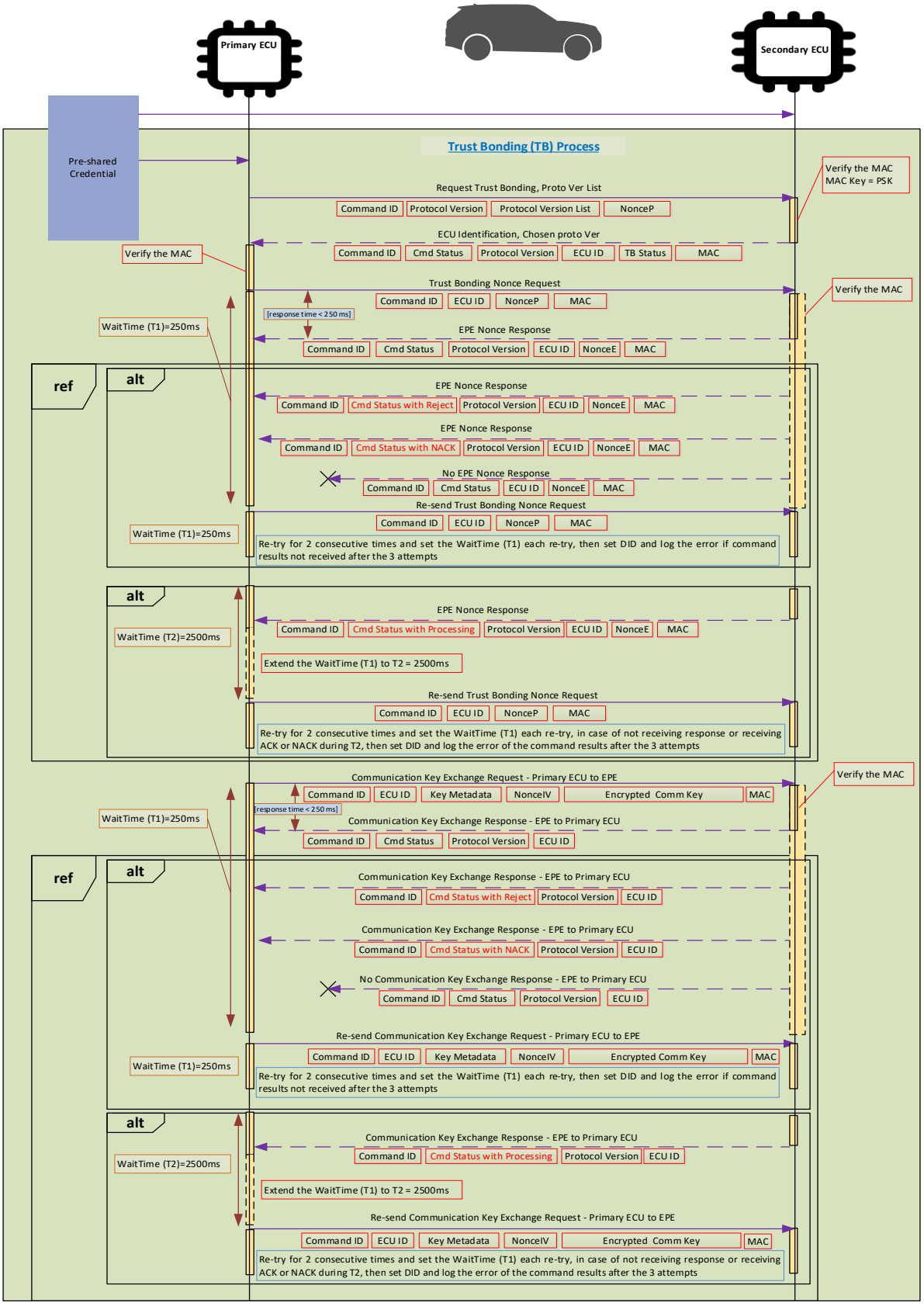


Figura 11 - Processo de Trust Bonding e de distribuição da Com Key

5.4.4 - Distribuição segura de mensagens em tempo

Finalmente, podemos apresentar a solução de ponta a ponta proposta para este projeto, que propõe uma abordagem segura para distribuir informações de tempo entre as ECUs no veículo. Para resumir o que é necessário para compartilhar o tempo de forma segura entre as ECUs, as seguintes fases devem ser alcançadas com êxito:

1. *Trust Bonding* deve ser realizado com êxito, incluindo a distribuição da Com Key única que será utilizada para garantir a mensagem segura de tempo.
2. Antes de qualquer distribuição segura de mensagens em tempo, o *Nonce* deve ser trocado com segurança entre os ECUs, para evitar contra-ataques de *replay*.

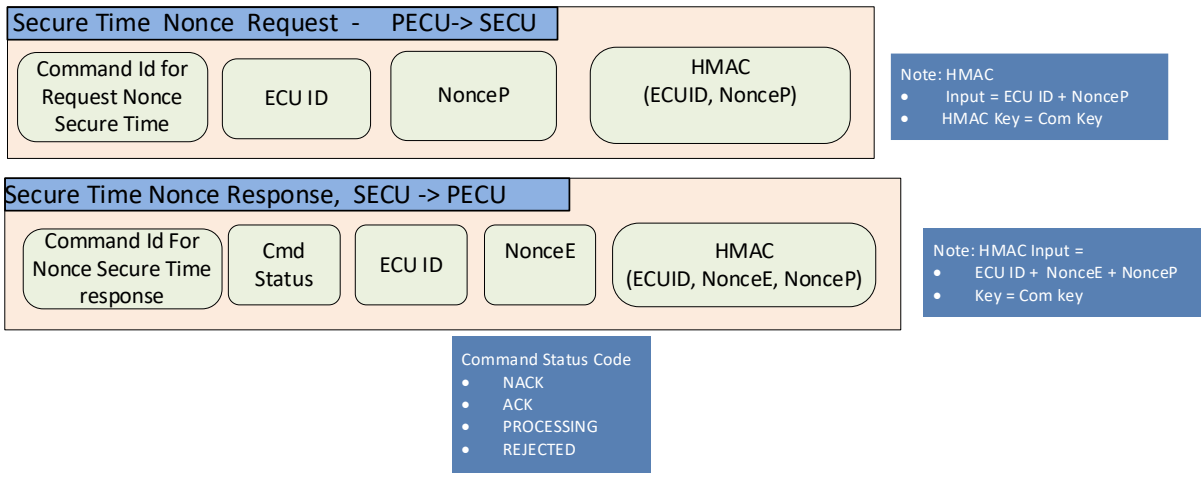


Figura 12 - Solicitação e respota de Tempo Seguro com Nonce

A SECU usará o tempo seguro recebido para validar os certificados. Esta será uma solicitação iniciada pela SECU quando necessário.

A Figura 12 mostra o fluxo resumido:

1. A SECU enviará um pedido de PECU para obter o tempo seguro quando precisar.
2. A SECU deve gerar um *nonce* para ser incluído com a solicitação de tempo seguro.

   Justificativa: Para evitar os ataques de *replay*.

3. A SECU deve incluir um campo de verificação de integridade na solicitação, HMAC.
4. A PECU deve verificar o campo de integridade antes de responder ao pedido.
5. A PECU deve gerar um *nonce* a ser incluído como parte da resposta em tempo seguro.
6. A PECU enviará o tempo em formato ASCII, como mostra a Figura 3.
7. O PECU deve proteger a mensagem usando o método de integridade, como o HMAC.
8. A SECU deve verificar a integridade ao receber a mensagem antes de confiar em usar o tempo atual para seu caso de uso.

A figura 13 mostra o processo de distribuição de tempo seguro entre a PECU e a SECU. O tempo deve ser incluído no MAC para fornecer Integridade e Autenticidade. Além disso, caso a SECU não tenha respondido com confirmação positiva, a PECU deve tentar novamente por duas vezes consecutivas e definir o tempo limite (250ms) a cada nova tentativa, e se a PECU não recebeu resposta, ACK ou NACK, ou *Rejected* após as 3 tentativas, então o campo de DID deve registra o erro do comando. O fluxo descrito na figura 13 poderá acontecer continuamente, sempre que a SECU precise da informação de tempo seguro, diferentemente do Trust Bonding que deverá acontecer durante a produção do veículo ou na substituição de uma das ECUs, em caso de defeito por exemplo.

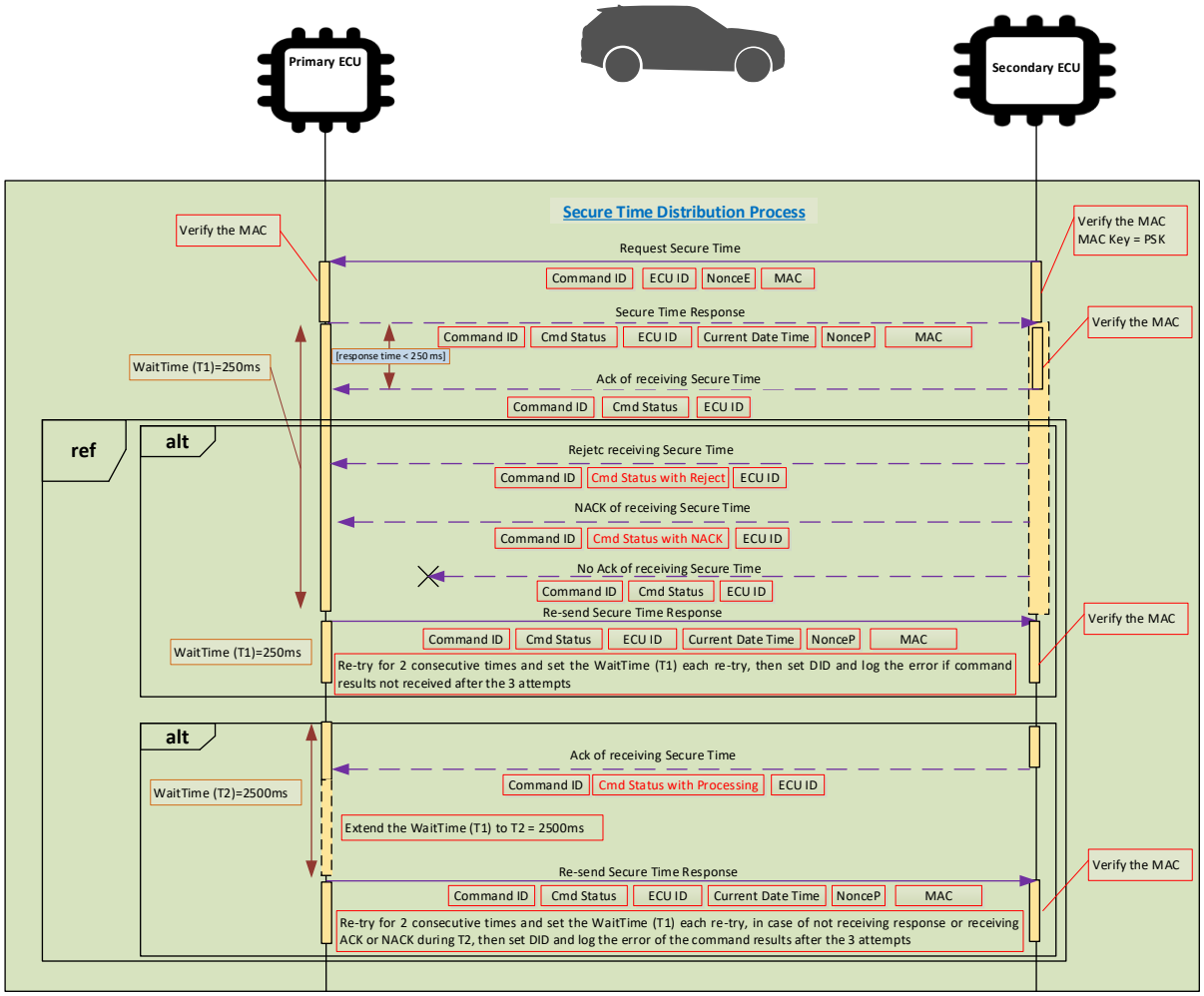


Figura 13 - Processo de distribuição de tempo seguro

Esse protocolo supera os obstáculos para as SECUs que não têm capacidade de solicitar o Tempo Seguro de uma fonte *off-board* segura. Além disso, minimiza o *overhead* na rede do veículo, mantendo o desempenho. Este protocolo alcança alta segurança fornecendo integridade e autenticação. Do ponto de vista da agilidade criptográfica, este protocolo é capaz de se adaptar e fazer a transição para diferentes algoritmos ou protocolos criptográficos, conforme necessário. O capítulo seguinte abordará a implementação do artefato, que deve nos permitir validar a solução proposta e a partir da análise nos dar resultados práticos em relação ao desempenho e resiliência de segurança.

5.5 - Implementação

Uma parte muito importante da metodologia DSR é a definição de um artefato que possa ser implementado e permitir a validação da solução teórica proposta. Abraçando a metodologia base para este trabalho, além do *mindset* das principais metodologias ágeis utilizadas atualmente durante o desenvolvimento da tecnologia, a ideia é identificar a forma mais simples e eficaz de implementar um artefato, ou protótipo, que permita analisar a solução e corrigir o projeto teórico, se necessário.

O artefato precisa abranger três etapas importantes para validar a solução proposta na seção anterior:

1) Permitir validar a implementação do protocolo proposto e, consequentemente, validar sua viabilidade.

2) Provar matematicamente que a solução proposta é resiliente contra os ataques mais relevantes neste ambiente, como manipulação de conteúdo, ataque de *replay*, propriedades e etc.

3) Garantir que a prova de conceito reflita o ambiente de implementação real e que as limitações da solução e as oportunidades de trabalho futuro possam ser compreendidas.

Na Figura 14, temos então o escopo pretendido pelo artefato. Em cinza temos as premissas que não serão implementadas:

1. A PECU tem acesso a uma fonte externa confiável para garantir que ela tenha uma informação de relógio confiável.
2. O PECU possui *hardware* com a capacidade de manter essas informações protegidas contra manipulação.

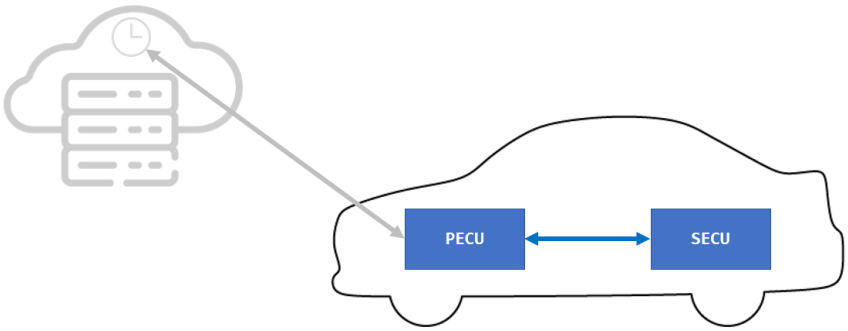


Figura 14 - Escopo do artefato

Em azul, temos então o escopo do artefato. Precisamos de uma entidade capaz de representar a PECU que tenha a fonte confiável de relógio dentro do veículo. Precisamos de outra entidade que represente a SECU que precise das informações para a validação segura do certificado. Finalmente, temos a ligação entre as duas entidades que representam diferentes tipos de tecnologia de rede presentes e como o protocolo entre as duas entidades pode satisfazer as particularidades para aquele ambiente.

Para a correta implementação do artefato, precisamos definir alguns parâmetros importantes do protocolo a ser validado. Para criar a relação de confiança entre PECU e SECU, será utilizada uma chave pré-compartilhada, simulando o que aconteceria durante o processo de fabricação do veículo.

Ao fazer uma solicitação de informações de tempo, a SECU envia uma mensagem para a PECU com uma ID de comando de 0x1F como mostra a Figura 15. O primeiro byte do campo ID da ECU é a ID da ECU que está enviando a solicitação e os 16 bytes a seguir são o número de série da ECU. O NonceE é um número aleatório de 8 bytes. O HMACkcomm é criptografado com a chave pré-compartilhada e contém o ID da ECU e o NonceE.

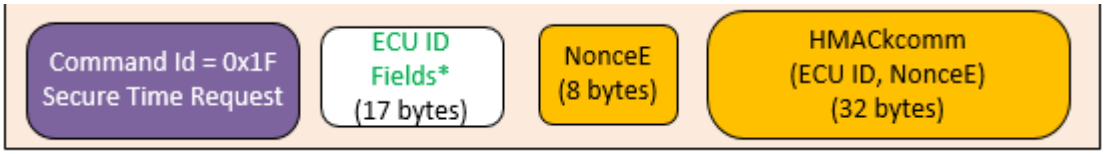


Figura 15 - Estrutura de mensagens de solicitação de tempo seguro para implementação do artefato

O PECU extrai cada campo na mensagem enviada pela SECU e descriptografa o HMAC para verificar sua integridade, verificando se ele corresponde ao HMAC verificado.

O PECU, então, solicitaria o tempo seguro ao servidor e responderia à SECU. A mensagem de resposta de atualização de tempo seguro tem uma ID de comando de 0x20 como mostrado na Figura 16. O campo de status Cmd é de 2 bytes e contém informações sobre se a solicitação foi reconhecida, rejeitada ou ainda está em processamento. Ack tem um código de status de 0x01, "*Processing*" tem um código de status de 0x02 e é usado em casos em que a resposta está demorando mais para enviar do que o tempo de vida da resposta de mensagem de tempo seguro. "*Rejected*" tem um código de status de 0x03. O campo ID da ECU é o mesmo da mensagem de solicitação e, em seguida, o campo de Tempo é um campo de 16 bytes.

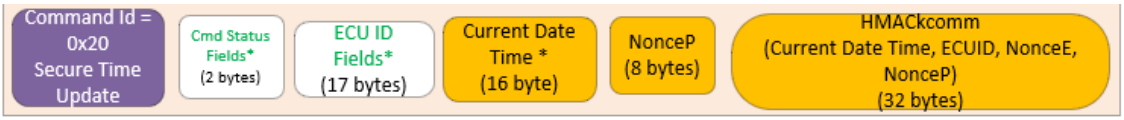


Figura 16 - Estrutura de mensagem de resposta de tempo seguro para implementação do artefato

O uso da metodologia DSR foi extremamente adequado para esse tipo de projeto de pesquisa, pois a sua proposta incremental foi vital para a avaliação dos quadros propostos e a definição do tamanho necessário para cada um deles de maneira eficaz só foi possível à partir de um número de interações permitindo a refinamento de detalhes específicos, como o tamanho necessário para a definição do tamanho do quadro de ID da ECU, inicialmente menor do que 17 bytes.

Para avaliar o desempenho e a viabilidade do protocolo proposto, foi proposta uma aplicação no mundo real, como mostra a Figura 17. Esta aplicação também ajudará a identificar potenciais desafios e áreas de melhoria. A entidade selecionada para representar o PECU aqui é uma ECU real da Jaguar Land Rover que tem todos os elementos necessários para simulá-lo:

- Conectividade externa através de LTE e WiFi.
- Informações de tempo provenientes do GPS.
- RTC interno para manter as informações do relógio.

- Trustzone de *hardware* da Qualcomm para executar operações de criptografia com segurança.
- Sistema operacional Linux rodando em uma VM (Virtual Machine) chamada "SOTA" na figura abaixo que pode receber a aplicação a ser implementada.

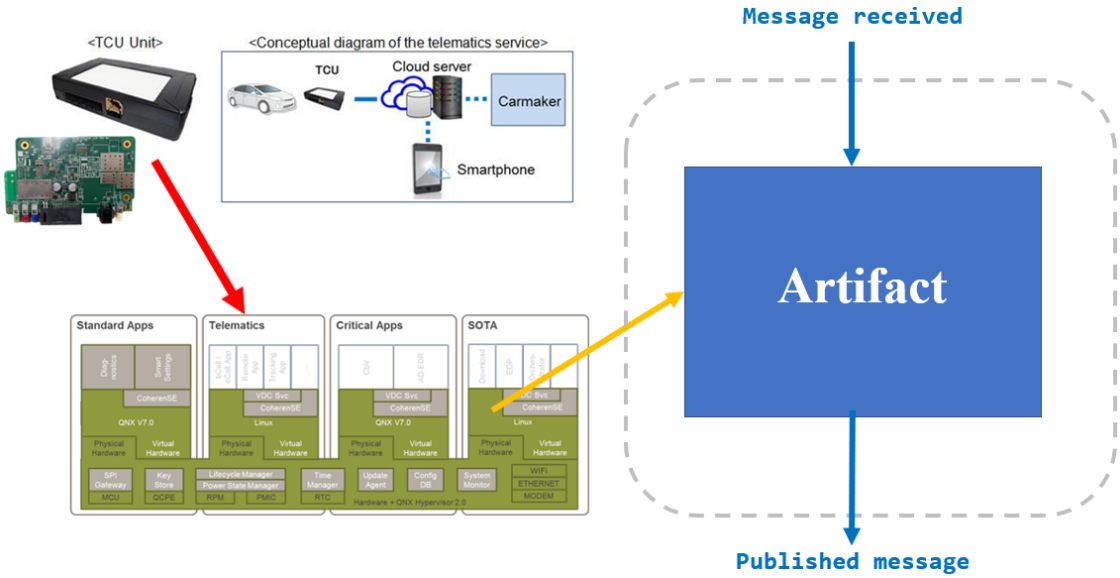


Figura 17 - Artefato proposto para avaliação do protocolo

Esta unidade tem privilégios de confiança e se conectará ao servidor recuperando o *timestamp* seguro e da rede BroadR-Reach com o protocolo descrito na seção anterior, transferirá o *timestamp* para a SECU. Como dito anteriormente, a PECU é uma ECU do mundo real que já contém o *software* compatível com o protocolo selecionado.

Para implementar o SECU, também estamos usando uma ECU real da Jaguar Land Rover, plataforma AutoSAR com todas as limitações que estamos destacando, como nenhum RTC para gerenciamento de tempo. A ECU é apresentada na figura 18 e receberá uma segunda aplicação de *software* para solicitar e receber as informações temporais da PECU. Para apoiar a aplicação do lado da SECU também temos a ferramenta automotiva Vector CANoe que ajuda na implementação de quadros de comunicação padrão.

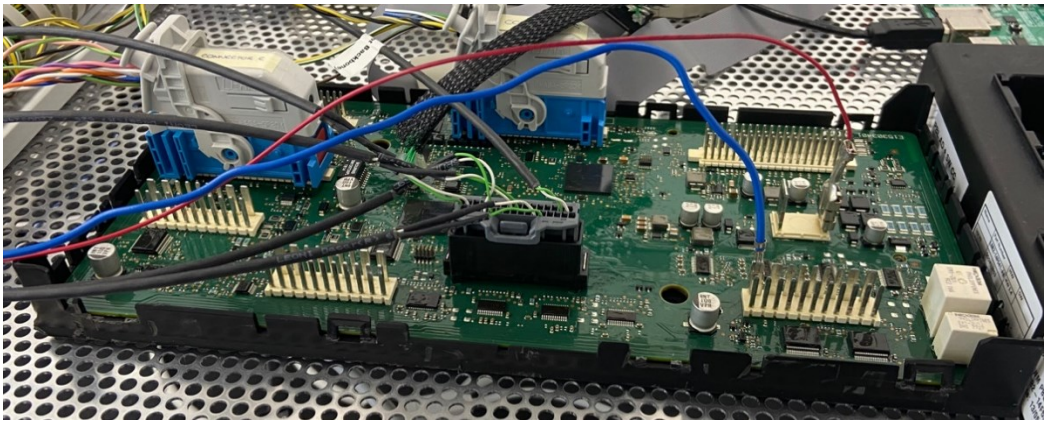


Figura 18 - Placa de ECU end point (SECU) com conexões necessárias para se comunicar

Para o recebimento da versão segura das informações do relógio, obtivemos a disponibilidade de um servidor que poderia compartilhar as informações de tempo com autenticação. Nos conectaremos ao servidor utilizando HTTP + TLS para consumo de uma API através de um arquivo *batch* que estabelecerá a conexão com o servidor, garantindo uma comunicação segura. Para fins de teste, a conexão com o servidor acontece pela rede WiFi.

Com base nas informações fornecidas pelo servidor, a comunicação requer pelo menos a aplicação OpenSSL versão 1.1.1, amplamente utilizada em soluções embarcadas que requerem operações criptográficas. No entanto, devido a dificuldades em instalar esta versão no PECU real, optamos por um Raspberry Pi 3 (Figura 19). O Raspberry Pi oferece poder computacional suficiente e seu *system-on-a-chip* é semelhante a uma ECU do mundo real, tornando o experimento razoavelmente significativo.

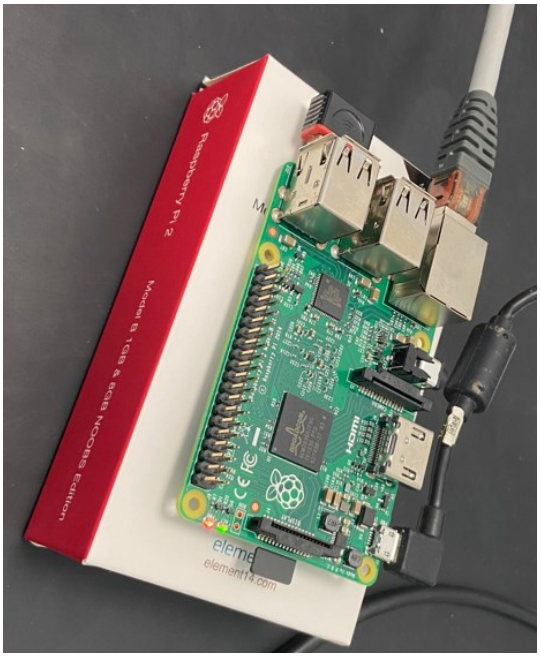


Figura 19 - Raspberry Pi para acesso ao servidor usado conectar com a PECU

No entanto, a PECU escolhida possui com um conector BroadR-Reach, enquanto o Raspberry Pi tem uma porta Ethernet 100Base-TX. Para preencher essa lacuna de conectividade, o Vector VN5640 (Figura 21) é usado como um dispositivo para conectar e monitorar a rede entre os dois dispositivos.

Finalmente, podemos ver na figura 20 o diagrama do artefato de ponta a ponta, mostrando o Raspberry conectado ao Servidor usando HTTP e conectado ao PECU via ethernet. PECU é conectado à SECU também via link ethernet.

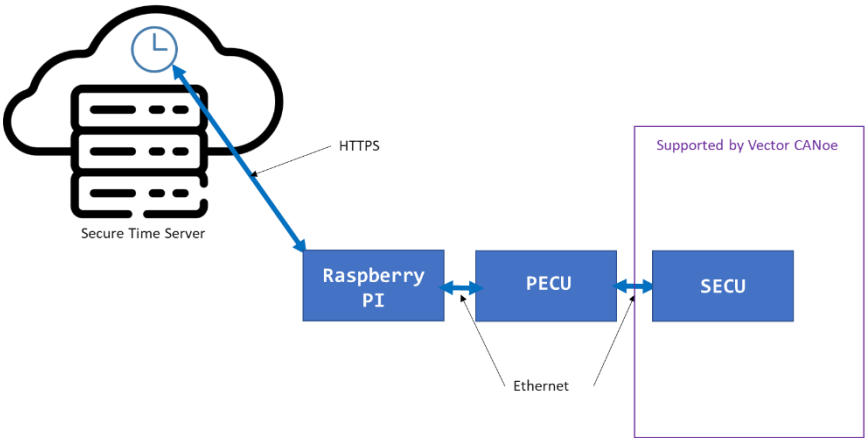


Figura 20 - Diagrama de implementação do artefato

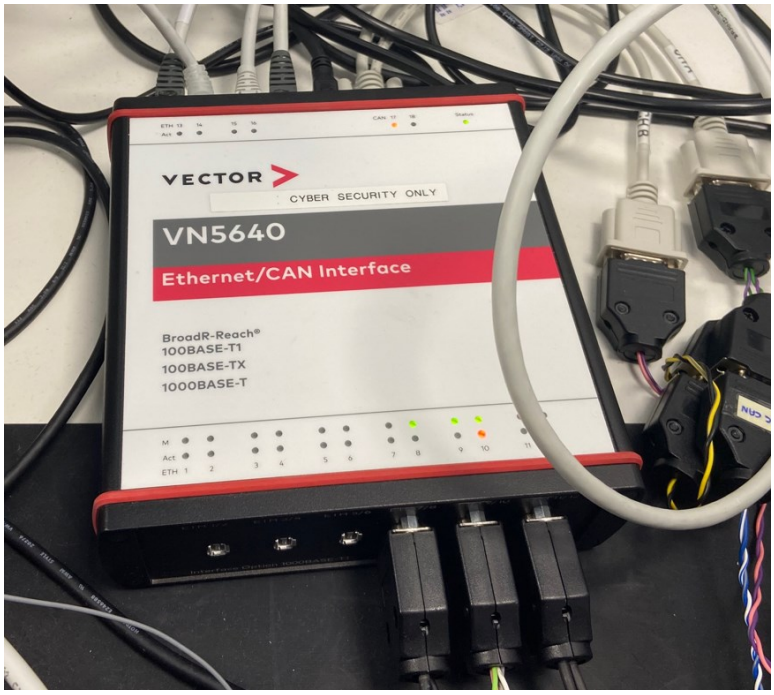


Figura 21 - Vector VN5640: Switch que permite a comunicação entre os dispositivos

Para executar os testes, a SECU foi previamente *Trust Bonded* e uma aplicação de *software* foi desenvolvida para o Raspberry PI. Este *software* é acionado pela mensagem *Secure Time Request* e está programado para responder com a mensagem Secure Time Response. Para fins de teste, apenas a resposta "ACK" foi implementada, se a mensagem for rejeitada, o Rasperry Pi simplesmente ignorará a solicitação. O campo ID da ECU será sempre o mesmo da mensagem de solicitação. A figura 22 mostra a configuração completa.

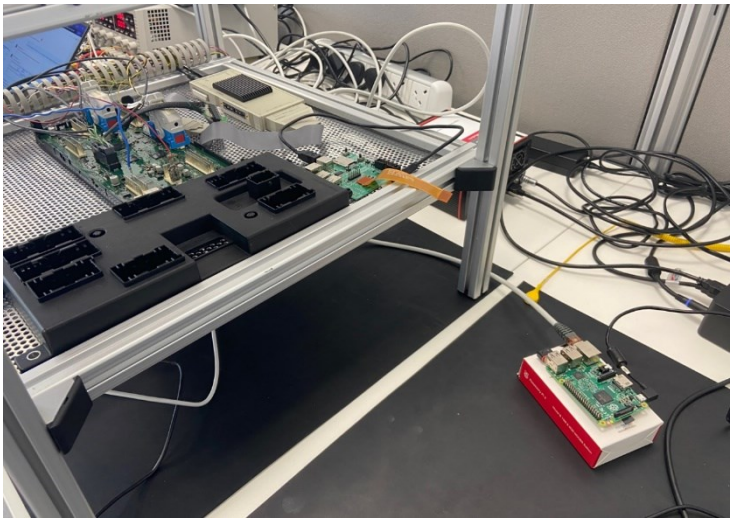


Figura 22 - Setup do artefato completo

Capítulo 6
Demonstração, Avaliação e Conclusões

6.1 - Demonstração

Esta seção demonstrará a funcionalidade do artefato implementado usando casos de uso específicos para isso. Inicialmente, a SECU solicitará tempo seguro ao PECU uma vez a cada um segundo. Portanto, para fins de teste, a SECU deixará de solicitar o tempo seguro quando a mensagem de hora segura for atualizada com êxito pelo Raspberry Pi. No entanto, na implementação real, a SECU tentará novamente por tempos específicos e, em seguida, acionará o DTC (flag de falha para diagnóstico), DIDs (memória de erro) e registrará o ERROR.

Para testar o artefato, conjuntos de casos de teste foram executados e logs para cada um foram gerados usando a ferramenta Wireshark. Os casos de teste são:

1. SECU recebe resposta válida de tempo seguro
2. HMAC inválido na resposta de tempo seguro:
    I. HMAC está incorreto.
    II. Os dados de tempo estão incorretos.

Primeiro caso de teste : SECU recebe resposta válida em tempo seguro

A Figura 23 mostra os logs da SECU que continuam solicitando o tempo seguro até receber uma resposta válida. A SECU validou a mensagem Secure Time comparando o HMAC recebido com o HMAC calculado. A SECU interromperá o envio de solicitações após receber uma resposta válida em tempo seguro.

No.	Time	Source	Destination	Protocol	Length	Info	Data
1	0.000000				140	<Ignored>	
2	1.009657	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
3	1.009991				140	<Ignored>	
4	2.019646	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
5	2.019973				140	<Ignored>	
6	3.029644	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
7	3.029966				140	<Ignored>	
8	4.039632	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
9	4.040018				140	<Ignored>	
10	5.049631	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
11	5.049986				140	<Ignored>	
12	6.059619	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935307667 30ea944586fa84…
13	6.061453	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303038…

Figura 23 - Rede monitorada com mensagens adequadas de Solicitação e Resposta de Tempo Seguro

A mensagem de *Secure Time Request* contém o seguinte *payload*:

- RX_PDU: 000002000000003a
- RX_CMD_ID: 1f
- RX_ECU_ID: 03000000000000353637303030323039 35
- RX_NONCE_E: b69683651ce1de22
- RX_HMAC:
  65e899fcc15f8f143050700ee3e26b5c4c5485103a7c10ea0ebd9174a582ea63

A mensagem *Secure Time Response* contém o seguinte *payload*:

- TX_PDU: 000002010000004c
- TX_CMD_ID: 20
- TX_CMD_STATUS: 0100
- TX_ECU_ID: 03000000000000353637303030323039 35
- TX_DATETIME: 00003230323330313330313835393032 (30/01/2023 18:59:02 – in yyyymmddhhmmss ascii format)
- TX_NONCE_P: 831538fbf09afe62
- TX_HMAC:
  71e75a84b1887ccf65aaba02af9b858c76ff779b25b85403374b83d2a5efc373

Segundo caso de teste: SECU recebe resposta de tempo seguro inválida

I. Cenário um: HMAC inválido na resposta de tempo seguro

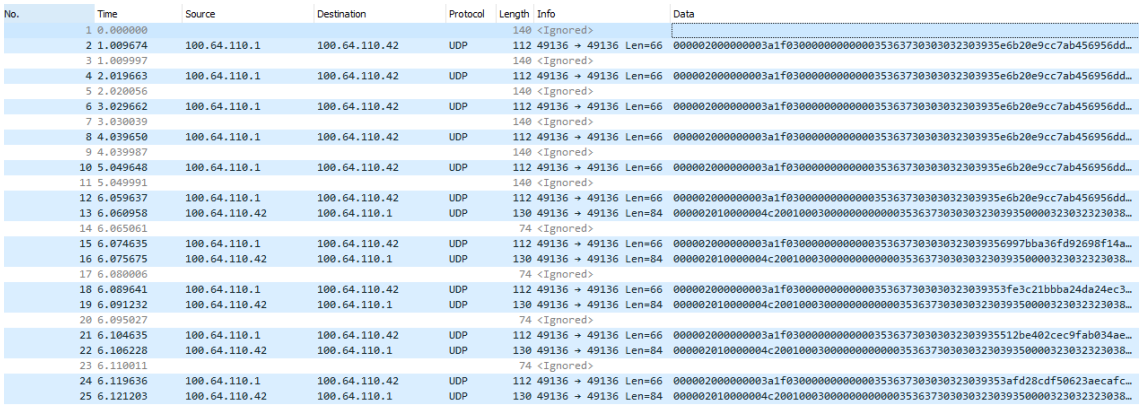
Declaração do problema: A SECU não conseguiu verificar a resposta de tempo seguro da PECU.

O HMAC pode ser inválido devido a uma das seguintes informações estarem incorretas:

- Current Time
- Communication Key
- NonceP
- NonceE

- ECU ID

Nesse caso de teste, o HMAC na resposta de tempo seguro é manipulado para um valor inválido. A mensagem é estruturada com HMAC incorreto para fins de teste. Portanto, mesmo que a PECU estivesse respondendo à solicitação com uma atualização de tempo seguro, a SECU continua solicitando uma resposta. A Figura 24 ilustra que a SECU continua solicitando o tempo seguro da PECU toda vez que recebe HMAC incorreto. A SECU comparará o HMAC calculado com o HMAC recebido cada vez que a resposta de tempo seguro recebida da PECU.



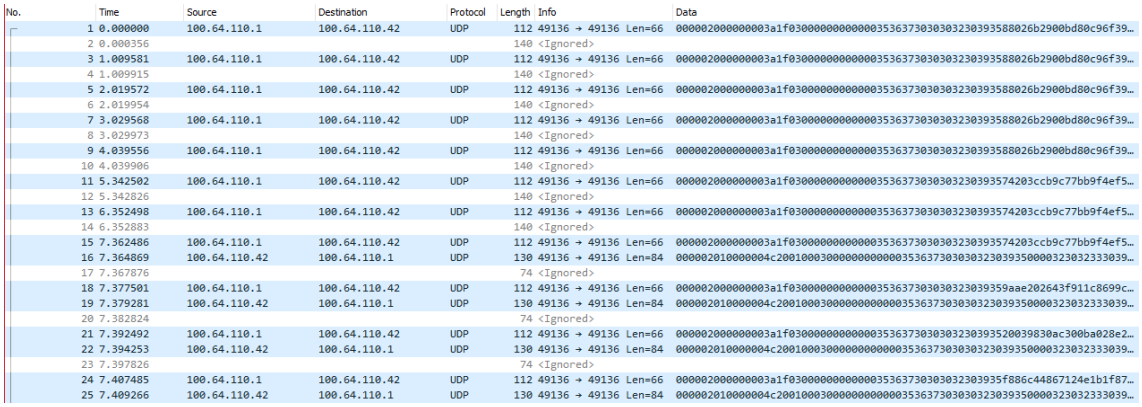
No.	Time	Source	Destination	Protocol	Length	Info	Data
1	0.000000				140	<Ignored>	
2	1.009674	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
3	1.009997				140	<Ignored>	
4	2.019663	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
5	2.020056				140	<Ignored>	
6	3.029662	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
7	3.030039				140	<Ignored>	
8	4.039650	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
9	4.039987				140	<Ignored>	
10	5.049648	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
11	5.049991				140	<Ignored>	
12	6.059637	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935e6b20e9cc7ab456956dd…
13	6.060958	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000 3536373030303230 3935000032303232303…
14	6.065061				74	<Ignored>	
15	6.074635	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 39356997bba36fd92698f14a…
16	6.075675	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000 3536373030303230 3935000032303232303…
17	6.080006				74	<Ignored>	
18	6.089641	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 39353fe3c21bbba24da24ec3…
19	6.091232	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000 3536373030303230 3935000032303232303…
20	6.095027				74	<Ignored>	
21	6.104635	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 3935512be402cec9fab034ae…
22	6.106228	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000 3536373030303230 3935000032303232303…
23	6.110011				74	<Ignored>	
24	6.119636	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000 3a1f03000000000000 3536373030303230 39353afd28cdf50623aecafc…
25	6.121203	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000 3536373030303230 3935000032303232303…

Figure 24 - Rede monitorada com HMAC incorreto da SECU

II. Cenário dois: Tempo de dados atual inválido na resposta de tempo seguro

Instrução do problema: A hora de dados atual não está correspondendo ao HMAC.

Neste caso de teste, a SECU enviou uma solicitação de tempo seguro para a PECU, então a PECU respondeu com o HMAC correto, mas a data da hora atual é diferente da hora real codificada no HMAC. Como resultado, a data de hora atual fornecida é inválida, a SECU rejeita a mensagem e continua solicitando a hora segura.



No.	Time	Source	Destination	Protocol	Length	Info	Data
1	0.000000	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935880 26b2900bd80c96f39…
2	0.000356				140	<Ignored>	
3	1.009581	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935880 26b2900bd80c96f39…
4	1.009915				140	<Ignored>	
5	2.019572	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935880 26b2900bd80c96f39…
6	2.019954				140	<Ignored>	
7	3.029568	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935880 26b2900bd80c96f39…
8	3.029973				140	<Ignored>	
9	4.039556	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935880 26b2900bd80c96f39…
10	4.039906				140	<Ignored>	
11	5.342502	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935742 03ccb9c77bb9f4ef5…
12	5.342826				140	<Ignored>	
13	6.352498	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935742 03ccb9c77bb9f4ef5…
14	6.352883				140	<Ignored>	
15	7.362486	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935742 03ccb9c77bb9f4ef5…
16	7.364869	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000035363730303032303935000032303233303 9…
17	7.367876				74	<Ignored>	
18	7.377501	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935 9aae202643f911c8699c…
19	7.379281	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000035363730303032303935000032303233303 9…
20	7.382824				74	<Ignored>	
21	7.392492	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935 20039830ac300ba028e2…
22	7.394253	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000035363730303032303935000032303233303 9…
23	7.397826				74	<Ignored>	
24	7.407485	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	00000200000000003a1f0300000000000035363730303032303935 f886c44867124e1b1f87…
25	7.409266	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	00000201000000 4c20010003000000000000035363730303032303935000032303233303 9…

Figura 25 - Rede monitorada com timestamp incorreto da SECU

6.2 - Avaliação

Para a correta avaliação do funcionamento do artefato, serão consideradas as três principais questões levantadas durante a seção de implementação do capítulo 5, a fim de refletir sobre o que foi desejado versus o que foi coletado durante a demonstração do capítulo anterior.

O primeiro ponto diz respeito à validação da viabilidade do protocolo a ser implementado. A partir dos requisitos detalhados inseridos no protocolo, como o número de bytes de cada campo e *payload* da mensagem, foi possível implementar o protocolo e acompanhar a execução do *handshake* entre as centrais. Como visto na figura 24, o comprimento das mensagens nunca foi maior do que 130 bytes.

No.	Time	Source	Destination	Protocol	Length	Info	Data
1	0.000000				140	<Ignored>	
2	1.009674	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
3	1.009997				140	<Ignored>	
4	2.019663	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
5	2.020056				140	<Ignored>	
6	3.029662	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
7	3.030039				140	<Ignored>	
8	4.039650	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
9	4.039987				140	<Ignored>	
10	5.049648	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
11	5.049991				140	<Ignored>	
12	6.059637	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935e6b20e9cc7ab456956dd…
13	6.060958	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303…
14	6.065061				74	<Ignored>	
15	6.074635	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935 6997bba36fd92698f14a…
16	6.075675	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303…
17	6.080006				74	<Ignored>	
18	6.089641	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935 3fe3c21bbba24da24ec3…
19	6.091232	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303…
20	6.095027				74	<Ignored>	
21	6.104635	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935 512be402cec9fab034ae…
22	6.106228	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303…
23	6.110011				74	<Ignored>	
24	6.119636	100.64.110.1	100.64.110.42	UDP	112	49136 → 49136 Len=66	000002000000003a1f0300000000000035363730303032303935 3afd28cdf50623aecafc…
25	6.121203	100.64.110.42	100.64.110.1	UDP	130	49136 → 49136 Len=84	000002010000004c2001000300000000000035363730303032303935000032303232303…

Figura 26 - Rede monitorada com quadro HMAC incorreto

O segundo ponto estava relacionado à prova de que o protocolo seria resiliente contra-ataques reais de manipulação de quadros. Como vimos em casos de uso em que o conteúdo da mensagem não corresponde ao HMAC calculado, a SECU prontamente rejeitou a mensagem, demonstrando assim sua resiliência contra esse tipo de ataque de adulteração de valor de tempo. O mesmo acontece quando o HMAC é alterado, a SECU também não aceita a mensagem e solicita uma nova. Esse resultado também é mostrado na figura 24 após a linha 13.

Finalmente, o terceiro ponto diz respeito a se o artefato reflete uma implementação real. Vimos que durante a implantação, essa foi uma preocupação constante, buscando apesar dos desafios, chegar o mais próximo possível do que seria

encontrado em um veículo moderno. Foram utilizados ECUs reais, que refletem a realidade atual de uma central com mais recursos, com máquinas virtuais, SO e *hardware* com recursos de segurança, e do outro lado uma central mais simples em termos de recursos, com arquitetura de *software* AutoSAR. As duas centrais estão conectadas por uma verdadeira rede *ethernet* automotiva e as ferramentas utilizadas são profissionais do universo automotivo. A prova de conceito com o rigor executado seria, sem dúvida, reutilizada dentro da indústria para uma implementação real como próximo passo a ser realizado.

6.3 - Conclusões

Este trabalho destacou alguns dos desafios de cibersegurança enfrentados pela indústria automotiva à medida que avança em direção a um mundo mais conectado e autônomo. Isso junto com as regulamentações como a UNECE R155 fez com que as montadoras projetassem controles de segurança que reduzissem os riscos de ataques cibernéticos. Um aspecto importante da proteção da segurança é provar a autenticidade e a validação dos certificados criptográficos, pois a postura geral de segurança depende da autenticação das partes finais. Uma vez que o veículo é uma rede distribuída de ECUs e apenas alguns dos ECUs estão ligados, o principal desafio é dispor de uma fonte de tempo segura para a validação dos certificados apresentados aos diferentes ECUs dentro do automóvel. Este artigo analisou as literaturas existentes e constatou que hoje não existe uma abordagem padronizada para distribuir o tempo com segurança para as UCE. O artigo propôs um método de distribuir o tempo de forma segura para ECUs sem conectividade com fonte de tempo externa ou RTC. O projeto proposto primeiro estabeleceu uma relação de confiança entre PECU e SECU através da distribuição de uma chave de comunicação única criptografada e MAC protegida através de um PSK. O método é altamente seguro em termos da propriedade de segurança de integridade e autenticidade dos dados de tempo que estão sendo distribuídos. O método proposto também leva em conta a agilidade cripto, já que os carros estão em campo há mais de 15 anos e o protocolo definido tem capacidade de mudar para um algoritmo mais recente por meio da atualização das versões cripto.

Para provar que o método proposto atende aos seus objetivos de segurança, os protocolos foram implementados em uma PECU e SECU representativas para distribuir e receber tempo com segurança. A implementação foi nos componentes de *hardware* onde todas as restrições são levadas em conta, como a operação segura, algoritmos e a capacidade da rede.

A implementação de um protótipo para validar uma proposta de informação de tempo seguro (clock) para verificação de certificados criptográficos embarcados em um veículo enfrentou uma série de desafios técnicos complexos, sendo o principal deles a

disparidade de plataformas entre as ECUs. Na ECU principal, dotada de um processador MCU potente, operava-se um hypervisor com máquinas virtuais em Linux, proporcionando um ambiente robusto e flexível para o desenvolvimento e teste do código em linguagem C. Essa configuração, similar a um smartphone moderno, permitia uma abordagem mais convencional de desenvolvimento e depuração, facilitando a implementação de algoritmos criptográficos e protocolos de comunicação. Por outro lado, a ECU secundária, equipada com um processador mais limitado, operava um código significativamente mais simples utilizando a plataforma AutoSAR. Aqui, as aplicações eram geradas a partir de modelos Matlab, introduzindo uma camada adicional de complexidade devido à natureza não convencional do processo de desenvolvimento. A integração desses sistemas heterogêneos representou um desafio considerável, uma vez que pequenas diferenças de implementação resultaram em problemas significativos de depuração, especialmente na implementação do HMAC, onde as nuances de funcionamento entre as plataformas exigiram ajustes delicados.

Além disso, a interação da ECU principal com a *Trustzone* da Qualcomm para os cálculos criptográficos adicionou uma camada adicional de complexidade ao projeto. A *Trustzone*, como um ambiente seguro isolado, exigia uma compreensão profunda de seu funcionamento interno, bem como das interfaces de programação de aplicativos (APIs) disponíveis para interação com o hardware subjacente. Isso envolveu a integração cuidadosa com o cryptoHAL (Hardware Abstraction Layer), que fornece uma interface padronizada para operações criptográficas de baixo nível. A necessidade de conhecimento especializado em criptografia, juntamente com a compreensão dos requisitos específicos da *Trustzone*, tornou a implementação e depuração dos algoritmos criptográficos particularmente desafiadoras. Em suma, a complexidade técnica envolvida na integração de diferentes plataformas, juntamente com a interação com tecnologias de segurança avançadas como a *Trustzone*, destacou a importância de uma abordagem meticulosa e altamente técnica para o desenvolvimento bem-sucedido de sistemas embarcados críticos para segurança.

Os resultados dos casos de teste mostraram que a SECU não aceitou um tempo que falhou na verificação de integridade e continuou solicitando tempo seguro. Os resultados também indicaram que, se a mensagem de tempo seguro fosse inconsistente, os dados eram rejeitados. Outra classe de teste realizada foi usar uma técnica de troca de *nonce* para evitar ataques de repetição, onde ambos os ECUs verificarão a atualização da mensagem cada vez que o tempo seguro for solicitado. Além de incluir a ID da ECU no HMAC, isso fornecerá a autenticidade da ECU. Portanto, os resultados mostram que o método proposto atende aos objetivos de segurança de proteção de autenticidade e integridade definidos durante a seção de definição do problema.

Os resultados obtidos na prova de conceito (PoC) destacam a necessidade premente de investimento em pesquisas adicionais para aprimorar e otimizar o projeto conceitual, especialmente ao escalar o esquema de protocolo para acomodar um grande número de ECUs. Durante o desenvolvimento, tornou-se evidente que o sistema enfrenta limitações significativas em termos de sua capacidade de escalabilidade para lidar com múltiplas ECUs solicitando tempo seguro, o que pode resultar em erros de sincronização da máquina de estado dentro da PECU. Esta constatação ressalta a importância de um aprofundamento na pesquisa para solucionar esses desafios, garantindo que o sistema possa lidar de forma eficaz com um ambiente operacional mais abrangente.

Um aspecto crucial que requer maior atenção é o aprimoramento do design de proteção contra repetição. Neste sentido, é essencial assegurar que os *nonces* sejam exclusivos e aleatórios, uma vez que as SECUs com recursos de memória e capacidade de processamento limitados enfrentam dificuldades para verificar a exclusividade dos *nonces* emitidos. Essa lacuna na verificação de *nonces* pode comprometer a segurança e a integridade do sistema em larga escala, exigindo uma abordagem cuidadosa e detalhada para resolver esse problema substancial. Embora tenhamos reconhecido essa limitação desde o início do projeto, optamos por direcionar nossos esforços para garantir a continuidade da solução desse desafio real e estamos comprometidos em trabalhar na implementação de sua escalabilidade em pesquisas futuras, visando uma abordagem mais abrangente e robusta para o sistema proposto.

A análise mais aprofundada revelou que o dimensionamento do esquema de protocolo para um grande número de ECUs apresenta desafios adicionais relacionados à latência e à sobrecarga de comunicação. A comunicação entre as ECUs deve ser coordenada de forma eficiente para evitar atrasos excessivos que possam comprometer a precisão do tempo seguro e a sincronização entre os dispositivos. Além disso, a integração dos algoritmos de verificação de certificados criptográficos em ambientes com recursos computacionais limitados requer uma abordagem cuidadosa para garantir um desempenho aceitável sem comprometer a segurança. A pesquisa futura deve se concentrar na otimização desses processos e na avaliação do impacto das limitações de recursos nas operações do sistema em escala.

No contexto das SECUs, a questão da verificação de *nonces* exclusivos revelou-se particularmente desafiadora. A geração de *nonces* exclusivos em ambientes com recursos limitados é uma tarefa complexa devido à falta de fontes confiáveis de entropia. A implementação de métodos eficazes para a geração e verificação de *nonces* exclusivos em SECUs representará um componente crucial para garantir a segurança e a integridade do sistema como um todo. Esse aspecto técnico exige uma abordagem interdisciplinar que combina conhecimentos de criptografia, engenharia de sistemas embarcados e protocolos de comunicação para desenvolver soluções robustas e eficazes.

Além disso, a questão da escalabilidade do sistema também levanta preocupações em relação à manutenção e gerenciamento de chaves criptográficas. À medida que o número de ECUs aumenta, torna-se cada vez mais desafiador gerenciar e atualizar as chaves de criptografia de forma segura e eficiente. A pesquisa futura deve abordar essa questão, desenvolvendo métodos e protocolos para distribuição segura de chaves e gerenciamento de políticas de segurança em ambientes complexos e distribuídos.

Em resumo, os resultados da PoC destacam a necessidade de pesquisas adicionais para resolver os desafios de escalabilidade e eficiência enfrentados pela proposta de informação de tempo seguro para verificação de certificados criptográficos embarcados em veículos. Esses desafios abrangem desde questões técnicas, como otimização de protocolos e algoritmos, até questões práticas relacionadas ao gerenciamento de chaves

e políticas de segurança. Ao abordar esses desafios de forma abrangente e interdisciplinar, podemos desenvolver soluções robustas e eficazes que atendam às demandas de segurança dos sistemas embarcados modernos.

Para concluir, este método proposto pode ser estendido para ser usado para necessidades semelhantes para os dispositivos IoT, produtos aeroespaciais e de automação industrial para atender às necessidades de distribuição de tempo segura. A pesquisa também indica a necessidade de ajudar a formular e padronizar a abordagem de segurança de alto nível para tempo seguro e incorporá-los por meio do AutoSAR e outros padrões automotivos conhecidos.

Referências

[1] C. Miller and C. Valasek, Remote exploitation of an unaltered passenger vehicle, *Black Hat USA*, vol. 2015, no. S 91 2015, pp. 1–91, 2015.

[2] W. UNECE, *Un regulation no. 155-cyber security and cyber security management system (2021)*. Disponível em: https://unece.org/transport/documents/2020/12/working-documents/grva-proposals-interpretation-documents-un-0.

[3] ISO 14229, *Road vehicles – unified diagnostic services (uds) – part 1: Application layer*, 2020. Disponível em: https://www.iso.org/standard/72439.html.

[4] ISO 15118-1, *Road vehicles — vehicle to grid communication interface — Part 1: General information and use-case definition, 2019.* Disponível em: https://www.iso.org/standard/69113.html

[5] Upstream Security – GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2023. Disponível em: https://upstream.auto/reports/global-automotive-cybersecurity-report/

[6] Guidelines for performing Systematic Literature Reviews in Software Engineering. Version 2.3. Software Engineering Group, School of Computer Science and Mathematics, Keele University and Department of Computer Science, University of Durham (2007)

[7] F. M. Anwar and M. B. Srivastava, A case for feedforward control with feedback trim to mitigate time transfer attacks, *ACM Trans. Priv. Secur.* [online], vol. 23, no. 2 2020, 11:1–
11:25, 2020.
Disponível em: https://doi.org/10.1145/ 3382503.

[8] R. Canetti, K. Hogan, A. Malhotra, and M. Varia, “A universally composable treatment of network time,” in *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*, IEEE Computer Society, 2017, pp. 360–375. Disponível em: https://doi.org/10.1109/CSF.2017.38.

[9] S. N. A. Ahmed, P. K. Meher, and A. P. Vinod, Efficient cross-correlation algorithm and architecture for robust synchronization in frame-based communication systems, *Circuits Syst.Signal Process.* [online], vol. 37, no. 6 2018, pp. 2548–2573, 2018. Disponível em: https://doi.org/10.1007/s00034-017-0678-3.

[10] P. Mundhenk, “Security for automotive electrical/electronic (E/E) architectures,” Ph.D. dissertation, Technical University Munich, Germany, 2017, ISBN: 978-3-7369-9604-5. Disponível em: https://d-nb.info/1138810037.

[11] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, “Lightweight authentication for secure automotive networks,” in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE*

2015, Grenoble, France, March 9-13, 2015, W. Nebel and D. Atienza, Eds., ACM, 2015, pp. 285–288. Disponível em: http: //dl.acm.org/citation.cfm?id=2755816.

[12] D. G. Berbecaru, S. Sisinni, A. Lioy, B. Rat, D. Margaria, and A. Vesco, Mitigating software integrity attacks with trusted computing in a time distribution network, *IEEE Access* [online], vol. 11 2023, pp. 50510–50527, 2023. Disponível em: https://doi.org/10.1109/ACCESS.2023.3276476.

[13] W. Zhai, L. Liu, Y. Ding, S. Sun, and Y. Gu, ETD: an efficient time delay attack detection framework for UAV networks, *IEEE Trans. Inf. Forensics Secur.* [online], vol. 18 2023, pp. 2913–2928, 2023. Disponível em: https://doi. org/10.1109/TIFS.2023.3272862.

[14] M. Langer and R. Bermbach, NTS4PTP - A comprehensive key management solution for PTP networks, *Comput. Networks* [online], vol. 213 2022, p. 109075, 2022. Disponível em: https://doi.org/10.1016/j.comnet.2022.109075.

[15] D. Kent, B. H. Cheng, and J. Siegel, Assuring vehicle update integrity using asymmetric public key infrastructure (pki) and public key cryptography (pkc), *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 2, no. 11-02-02-0013 2020, pp. 141–158, 2020.

[16] Z. Mahmood, A. Ullah, and H. Ning, Distributed multiparty key management for efficient authentication in the internet of things, *IEEE Access* [online], vol. 6 2018, pp. 29460–29473, 2018. Disponível em: https://doi.org/10. 1109/ACCESS.2018.2840131.

[17] Cebe, Mumin, "Efficient Key Management Schemes for Smart Grid" (2020). FIU Electronic Theses and Dissertations. 4460. Disponível em: https://digitalcommons.fiu.edu/etd/4460

[18] R. Annessi, J. Fabini, and T. Zseby, Securetime: Secure multicast time synchronization, *CoRR* [online], vol. abs/1705.10669 2017, 2017. Disponível em: http://arxiv.org/abs/1705.10669.

[19] M. Frei, J. Kwon, S. Tabaeiaghdaei, M. Wyss, C. Lenzen, and A. Perrig, “G-SINC: global synchronization infrastructure for network clocks,” in *41st International Symposium on Reliable Distributed Systems, SRDS 2022, Vienna, Austria, September 19-22, 2022*, IEEE, 2022, pp. 133–145. Disponível em: https://doi. org/10.1109/SRDS55811.2022.00021.

[20] M. Spanghero and P. Papadimitratos, “Detecting GNSS misbehavior leveraging secure heterogeneous time sources,” in *IEEE/ION Position, Location and Navigation Symposium, PLANS*
2023, Monterey, CA, USA, April 24-27, 2023, IEEE, 2023, pp. 996–1006. Disponível em: https://doi.org/10.1109/PLANS53410.2023.10140008.

[21] I. Fernandez-Hernandez, T. Walter, A. Neish, and C. O’Driscoll, “Independent time synchronization for resilient gnss receivers,” in *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, 2020, pp. 964–978.

[22] J. A. Sherman, L. Arissian, R. Brown, *et al.*, A resilient architecture for the realization and distribution of coordinated universal time to critical infrastructure systems in the United States: Methodologies and recommendations from the national institute of standards and technology (nist), *NIST Technical Note*, vol. 2187 2021, p. 189, 2021.

[23] K. Teichel, D. Sibold, and G. Hildermeier, "Delayed authentication and delayed measurement application in one-way synchronization," in *IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication, ISPCS 2018, Geneva, Switzerland, September 30 - October 5, 2018*, IEEE, 2018, pp. 1–6. Disponível em: https://doi.org/10.1109/ISPCS.2018.8543083.

[24] K. Teichel and G. Hildermeier, "Experimental evaluation of attacks on tesla-secured time synchronization protocols," in *Security Standardisation Research – 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings*, C. Cremers and A. Lehmann, Eds., ser. Lecture Notes in Computer Science, vol. 11322, Springer, 2018, pp. 37–55. Disponível em: https://doi.org/ 10.1007/978-3-030-04762-7%5C_3.

[25] M. Langer, K. Heine, D. Sibold, and R. Bermbach, "A network time security based automatic key management for ptpv2.1," in *45th IEEE Conference on Local Computer Networks,*
LCN 2020, Sydney, Australia, November 16-19, 2020, H. Tan, L. Khoukhi, and S. Oteafy, Eds., IEEE, 2020, pp. 144–153. Disponível em: https://doi.org/10.1109/LCN48667.2020.9314809.

[26] R. Annessi, J. Fabini, and T. Zseby, "It's about time: Securing broadcast time synchronization with data origin authentication," in *26th International Conference on Computer Communication and Networks, ICCCN 2017, Vancouver, BC, Canada, July 31 - Aug. 3, 2017*, IEEE, 2017, pp. 1–11. Disponível em: https://doi.org/10.1109/ICCCN.2017.8038418.

[27] K. O'Donoghue, D. Sibold, and S. Fries, "New security mechanisms for network time synchronization protocols," in *2017 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, IEEE, 2017, pp. 1–6.

[28] E. Kyriakakis, Time-predictable end-system design for real-time communication 2021, 2021.

[29] E. Itkin and A. Wool, A security analysis and revised security extension for the precision time protocol, *IEEE Trans. Dependable Secur. Comput.* [online], vol. 17, no. 1 2020, pp. 22–34, 2020. Disponível em: https://doi.org/10.1109/TDSC.2017.2748583.

[30] R. Annessi, J. Fabini, F. Iglesias, and T. Zseby, Encryption is futile: Delay attacks on highprecision clock synchronization, *CoRR* [online], vol. abs/1811.08569 2018, 2018. Disponível em: http://arxiv.org/abs/1811.08569.

[31] R. Kakade, J. Chou, and S. Torcato, Vulnerability analysis of time synchronization in automotive ethernet, *CoRR* [online], vol. abs/2208.11878 2022, 2022. Disponível em: https://doi.org/10.48550/arXiv. 2208.11878.

[32] H. J. Kim, U. Lee, M. Kim, and S. Lee, Time-synchronization method for can–ethernet networks with gateways, *Applied Sciences*, vol. 10, no. 24 2020, p. 8873, 2020.

[33] C. M. DeCusatis, R. M. Lynch, W. Kluge, J. Houston, P. A. Wojciak, and S. Guendert, Impact of cyberattacks on precision time protocol, *IEEE Trans. Instrum. Meas.* [online], vol. 69, no. 5 2020, pp. 2172–2181, 2020. Disponível em: https://doi.org/10.1109/TIM.2019.2918597.

[34] M. Langer, K. Teichel, D. Sibold, and R. Bermbach, "Time synchronization performance using the network time security protocol," in *2018 European Frequency and Time Forum (EFTF)*, IEEE, 2018, pp. 138–144.

[35] M. Langer, K. Heine, R. Bermbach, and D. Sibold, "Analysis and compensation of latencies in nts-secured ntp time synchronization," in *2020 Joint Conference of the IEEE International Frequency Control Symposium and International Symposium on Applications of Ferroelectrics (IFCS-ISAF)*, IEEE, 2020, pp. 1–10.

[36] M. Langer, K. Heine, R. Bermbach, and D. Sibold, "Extending the network time security protocol for secure communication between time server and key establishment server," in *2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS)*, IEEE, 2021, pp. 1–5.

[37] N. Tripathi and N. Hubballi, Preventing time synchronization in ntp's broadcast mode, *CoRR* [online], vol. abs/2005.01783 2020, 2020. Disponível em: https:// arxiv.org/abs/2005.01783.

[38] F. Mkacher, X. Bestel, and A. Duda, "Secure time synchronization protocol," in *IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication, ISPCS 2018, Geneva, Switzerland, September 30 - October 5, 2018*, IEEE, 2018, pp. 1–6.
Disponível em: https://doi.org/ 10.1109/ISPCS.2018.8543077.

[39] A. Malhotra and S. Goldberg, Attacking ntp's authenticated broadcast mode, *Comput. Commun. Rev.* [online], vol. 46, no. 2 2016, pp. 12–17, 2016. Disponível em: https://doi.org/10.1145/2935634.2935637.

[40] A. Malhotra, I. E. Cohen, E. Brakke, and S. Goldberg, "Attacking the network time protocol," in *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*, The Internet Society, 2016. Disponível em: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/ attacking-network-time-protocol.pdf.

[41] B. Dowling, D. Stebila, and G. Zaverucha, "Authenticated network time synchronization," in *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, T. Holz and S. Savage, Eds., USENIX Association, 2016, pp. 823–840. Disponível em:

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/dowling.

[42] M. Langer, T. Behn, and R. Bermbach, “Securing unprotected NTP implementations using an NTS daemon,” in *2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication, ISPCS 2019, Portland, OR, USA, September 22-27, 2019*, IEEE, 2019, pp. 1–6. Disponível em: https://doi.org/10.1109/ISPCS.2019.8886645.

[43] A. Malhotra, M. V. Gundy, M. Varia, H. Kennedy, J. Gardner, and S. Goldberg, “The security of ntp’s datagram protocol,” in *Financial Cryptography and Data Security – 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 10322, Springer, 2017, pp. 405–423. Disponível em: https://doi.org/10.1007/978-3-319-70972-7%5C_23.

[44] M. Langer, K. Teichel, K. Heine, D. Sibold, and R. Bermbach, “Guards and watchdogs in one-way synchronization with delay-related authentication mechanisms,” in *2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication, ISPCS 2019, Portland, OR, USA, September 22-27, 2019*, IEEE, 2019, pp. 1–6. Disponível em: https://doi.org/10. 1109/ISPCS.2019.8886633.

[45] T. He, Y. Zheng, and Z. Ma, Study of network time synchronisation security strategy based on polar coding, *Comput. Secur.* [online], vol. 104 2021, p. 102214, 2021. Disponível em: https://doi.org/10.1016/j.cose.2021. 102214.

[46] V. Vaishnavi, B. Kuechler: Design science research in information systems overview of design science research. Design Science Research in Information Systems and Technology (2004)

[47] ISO 11898-1 – *Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signaling, 2015.* Disponível em: https://www.iso.org/standard/63648.html

[48] Kitchenham, B. (2004). Evidence-Based Software Engineering and Systematic Reviews. Boca Raton, FL: Chapman & Hall/CRC.

[49] X.509: *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks". ITU. Retrieved 6 November 2019*. Disponível em: https://www.itu.int/rec/T-REC-X.509

[50] Foundations of Information Security: A Straightforward Introduction Paperback – 3 Oct. 2019 by Jason Andress (Author)

[51] Message Authentication using Hash Functions— The HMAC Construction. Mihir Bellare, Ran Canetti, Hugo Krawczyk – 1996. Disponível em: https://cseweb.ucsd.edu/~mihir/papers/hmac-cb.pdf

[52] Neuman, B.C. and Stubblebine, S.G. (1996). A Note on the Use of Tirnestamps as Nonces. Information Sciences Institute, University of Southern California.

[53] Advanced Encryption Standard (AES)

Morris J. Dworkin, Elaine B. Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, James F. Dray Jr., November 26, 2001. Disponível em: https://www.nist.gov/publications/advanced-encryption-standard-aes

[54] Cryptographic Key Generation: NIST Publishes SP 800-133 Rev. 2. June 04, 2020. Disponível em: https://www.nist.gov/news-events/news/2020/06/cryptographic-key-generation-nist-publishes-sp-800-133-rev-2

[55] SP 800-38F.

Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. December 2012 - Morris Dworkin (NIST)
Disponível em: https://csrc.nist.gov/publications/detail/sp/800-38f/final

[56] SP 800-38D

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. November 2007 - Morris Dworkin (NIST)
Disponível em: https://csrc.nist.gov/publications/detail/sp/800-38d/final