FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Kauê Urias de Bortoli

Natália Cristina Baltazar

SEGURANÇA EM *IoT*

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Kauê Urias de Bortoli
Natália Cristina Baltazar

Segurança em *IoT*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. José Luís Zem.

Área de concentração: Segurança da Informação em Internet das Coisas.

Americana, SP.
2023

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

BORTOLI, Kauê Urias de

Segurança em IoT. / Kauê Urias de Bortoli, Natália Cristina Baltazar – Americana, 2023.

44f.

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

Orientador: Prof. Dr. José Luís Zem

1. Internet das coisas 2. Segurança em sistemas de informação. I. BORTOLI, Kauê Urias de, II. BALTAZAR, Natália Cristina III. ZEM, José Luís IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681518
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Kauê Urias de Bortoli
Natália Cristina Baltazar

Segurança em *IoT*

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

Americana, 20 de junho de 2023.

Banca Examinadora:

José Luis Zem (Presidente)
Doutor
FATEC - Americana

Henri Alves de Godoy (Membro)
Doutor
FATEC - Americana

Benedito Luciano Antunes de França (Membro)
Mestre
FATEC - Americana

AGRADECIMENTOS

Em primeiro lugar expressamos nossa gratidão ao nosso orientador, pelo apoio e orientações valiosas ao longo deste processo.

Também gostaríamos de agradecer aos professores e profissionais da área que compartilharam seus conhecimentos e experiências por meio de palestras, cursos e materiais que nos enriqueceram e forneceram uma base sólida para o desenvolvimento deste trabalho.

Não podemos deixar de mencionar a contribuição dos nossos colegas de curso, que sempre estiveram dispostos a trocar ideias, discutir conceitos e fornecer sugestões construtivas. Agradecemos pelo apoio mútuo e pela parceria ao longo dessa jornada acadêmica.

À nossa família e amigos, que nos apoiaram incondicionalmente e nos encorajaram a buscar sempre o melhor, nosso mais profundo agradecimento. Suas palavras de encorajamento e compreensão foram fundamentais para superar os desafios e nos manter motivados.

Por fim, gostaria de expressar nossa gratidão um ao outro, por compartilhar essa jornada. Foi uma experiência enriquecedora trabalhar em conjunto, colaborando, dividindo tarefas e superando obstáculos. Nossa dedicação, comprometimento e visão complementar foram essenciais para o sucesso deste trabalho.

A todos que, de alguma forma, contribuíram para o desenvolvimento deste trabalho, nosso sincero agradecimento. Cada pessoa mencionada e aquelas que não foram citadas aqui tiveram um papel importante em nossa trajetória acadêmica. Estamos profundamente gratos pela oportunidade de realizar este trabalho e pelo apoio recebido ao longo do caminho.

DEDICATÓRIA

Dedicamos este trabalho a todas as pessoas que permaneceram ao nosso lado durante essa jornada acadêmica e nos apoiaram incondicionalmente. Em especial, gostaria de dedicar este trabalho aos nossos familiares e amigos, que foram fonte de incentivo e compreensão ao longo de todo o processo.

RESUMO

Este trabalho aborda a segurança em sistemas *IoT* por meio de práticas simuladas no PICSimLab. Seu objetivo é analisar os aspectos-chave da segurança, incluindo ataques de controle, intercepção de informação e interrupção de serviço. A metodologia empregada consiste na configuração do ambiente do simulador, no projeto de um sistema *IoT* simulado e na implementação da comunicação entre os dispositivos, utilizando protocolos adequados. Vulnerabilidades são identificadas e ataques controlados são realizados para explorar falhas de segurança e alterar o comportamento dos dispositivos. Além disso, um *sniffer* de rede é implementado para capturar e analisar pacotes de dados, identificando informações sensíveis e padrões de comunicação. Os resultados são avaliados, destacando os riscos e as ameaças identificadas. Com base nessa análise, medidas de segurança e recomendações são discutidas para mitigar essas ameaças em um ambiente real. Recomenda-se a utilização de criptografia robusta para proteger a transmissão de dados e a adoção de tecnologias atuais, como a computação em nuvem distribuída, para melhorar o desempenho e a análise em tempo real dos dados. O trabalho conclui ressaltando a importância de considerar a segurança em sistemas *IoT* e destaca a necessidade contínua de pesquisa e desenvolvimento de estratégias de segurança robustas para garantir a confidencialidade, integridade e disponibilidade desses sistemas. No contexto atual de rápida evolução tecnológica, é fundamental que os fabricantes e as empresas adotem abordagens proativas de segurança da informação, implementando protocolos adequados, atualizando regularmente os dispositivos e promovendo conscientização sobre os riscos associados aos dispositivos *IoT*.

Palavras-Chave: Segurança; Internet das coisas; Vulnerabilidades.

ABSTRACT

This paper addresses security in IoT systems through simulated practices in PICSimLab. Its objective is to analyze key aspects of security, including control attacks, information interception, and service disruption. The methodology employed involves configuring the simulator environment, designing a simulated IoT system, and implementing communication between devices using appropriate protocols. Vulnerabilities are identified, and controlled attacks are performed to exploit security flaws and alter device behavior. Additionally, a network sniffer is implemented to capture and analyze data packets, identifying sensitive information and communication patterns. The results are evaluated, highlighting the identified risks and threats. Based on this analysis, security measures and recommendations are discussed to mitigate these threats in a real-world environment. The use of robust encryption to protect data transmission and the adoption of current technologies, such as distributed cloud computing, to enhance performance and real-time data analysis are recommended. The paper concludes by emphasizing the importance of considering security in IoT systems and highlighting the ongoing need for research and development of robust security strategies to ensure confidentiality, integrity, and availability of these systems. In the current context of rapid technological advancement, it is crucial for manufacturers and companies to adopt proactive approaches to information security by implementing appropriate protocols, regularly updating devices, and promoting awareness of the risks associated with IoT devices.

Keywords: *Security; Internet of Things; Vulnerabilities.*

SUMÁRIO

LISTA DE FIGURAS

INTRODUÇÃO

De acordo um estudo realizado pela TGT Consult e a Associação Brasileira de Internet das Coisas (ABINC), até 2025 mais de 27 bilhões de dispositivos estarão conectados à internet e compartilhando informações. Esse conglomerado de conexões recebe o nome de Internet das Coisas (*Internet of Things - IoT*). Atualmente, grande parte destes dispositivos são utilizados para apoiar diversos modelos de negócios, devido a possibilidade de interação de equipamentos sem a dependência de usuários, permitindo a operação de uma rede de máquinas capazes de circular informações entre si e operarem de forma autônoma para tomada de decisões.

No entanto, a existência de uma rede de computadores com interação de dispositivos interconectados de forma tão extensa, apresenta diversos desafios na área de segurança, privacidade e integridade, tornando-se mais expostas a ataques e vulnerabilidades, visto que a infraestrutura neles apresentada é variável, possuindo em sua maioria recursos limitados, como baixa energia, capacidade de processamento e armazenamento restrita, conexão através de enlaces que possuem perdas, entre outras características.

Diante disso, questiona-se: Como melhorar a performance de segurança de dados e informações, em dispositivos *IoT*?

A metodologia a ser utilizada, a priori, envolve pesquisa bibliográfica, pesquisa documental e levantamento e análise de dados, disponíveis em sites e publicações técnicas e especializadas. Além disso, como parte prática deste estudo, será realizada a criação de um ambiente de teste, utilizando um dispositivo *IoT*, com o objetivo de simular situações reais e realizar ataques controlados. Esse ambiente permitirá a identificação e análise de possíveis vulnerabilidades e avaliação da eficácia das soluções de segurança integradas.

Este estudo tem como objetivo geral analisar conceitualmente as soluções de segurança e privacidade que podem ser integradas por organizações que usam *IoT* em seus negócios. Os objetivos específicos consistem em realizar pesquisa bibliográfica sobre segurança da informação e *IoT*, levantar dados em fontes abertas, como publicações técnicas, coletar e analisar informações sobre negócios que utilizam *IoT* e os respectivos riscos, bem como criar um ambiente de teste com um dispositivo *IoT* e realizar ataques controlados para avaliar a segurança do sistema.

Constata-se relevante a pesquisa a fim de compreender as vulnerabilidades aos quais as empresas estão sujeitas através da utilização de *IoT*, de modo a analisar soluções para as necessidades presentes nos aspetos de segurança e privacidade.

2 REVISÃO BIBLIOGRÁFICA

O capítulo apresenta a definição e os principais recursos da *IoT*, enfatizando sua aplicação em automação residencial, otimização industrial e monitoramento da saúde.

No entanto, também são destacados os riscos de segurança, como a necessidade de criptografar os dados transmitidos pelos dispositivos *IoT* e a vulnerabilidade dos dispositivos mal protegidos a ataques cibernéticos.

As bases utilizadas para a revisão bibliográfica consistem em livros de pesquisadores da tecnologia IoT e da área de Segurança da Informação, além de publicações científicas e sites. O período de publicação dos materiais utilizados consiste entre 2012 e 2022.

Os desafios relacionados ao endereçamento dos dispositivos *IoT* são explorados, considerando a compatibilidade com o endereçamento existente. Outro desafio é o gerenciamento eficiente do grande volume de dados gerados pelos dispositivos *IoT*, incluindo a necessidade de largura de banda adequada e análise de tráfego em grandes volumes de informações.

Por fim, são apresentados os riscos decorrentes da utilização da *IoT*, como ataques de controle, roubo de informações e interrupção de serviços. Exemplos de ataques cibernéticos, como o *botnet* Mirai, são mencionados para ilustrar esses riscos.

Em suma, o capítulo fornece uma visão geral dos conceitos, benefícios, riscos e desafios da *IoT*, destacando a importância de medidas de segurança e estratégias eficientes para mitigar os problemas enfrentados nesse campo.

2.1 Segurança da Informação

Embora, atualmente, o valor da informação seja mais reconhecido e comentado, a prática de segurança da informação é realizada desde muito tempo nas mais diversas civilizações. Na antiga China, por exemplo, a linguagem escrita era específica a membros pertencentes à classe superior que exerciam o direito de aprender a ler e a escrever. Utilizavam também de algumas formas distintas de registrar suas informações de acordo com seu grau de relevância, a escrita demótica, utilizada para os assuntos do cotidiano, e a hieroglífica, mais complexa e formada por

desenhos e símbolos, era usada para informações consideradas restritas a um grupo de pessoas (MASCARENHAS NETO; ARAÚJO, 2009).

Na Roma antiga, com diversas disputas por território, uma intercepção de mensagem podia significar essa perda de territórios. Com isso, houve uma das primeiras incursões no campo da criptografia com as cifras de César, que utilizava um sistema simples de substituição de algarismo que protegia as mensagens enviadas pelo Imperador Júlio César aos seus generais que estavam nos campos de batalha (MASCARENHAS NETO; ARAÚJO, 2009).

Nesse contexto histórico, houve um fato que talvez tenha sido o mais importante e representativo que é a construção da máquina Enigma, a qual foi utilizada pelos exércitos alemães durante a segunda guerra mundial para codificar e decodificar informações repassadas para suas tropas. A máquina era utilizada com o intuito de manter o sigilo das informações, para isso sua chave era alterada diariamente para dificultar a decodificação (MASCARENHAS NETO; ARAÚJO, 2009).

Na atualidade, vivencia-se um novo paradigma informacional, impulsionado pela evolução tecnológica, em que os conceitos de informação, conectividade e interatividade impõem grandes desafios às organizações. As informações tornaram-se acessíveis a qualquer momento, o conceito de fronteira foi alterado por uma nova realidade digital, e a tecnologia da informação perpetuou-se imputando o surgimento de novos comportamentos em relação às informações.

Para Wagner Araújo (2009, p.36),

> no mundo conectado em rede, onde a informação flui, as organizações, sejam empresas privadas ou do setor governamental, necessitam de processos e controles de segurança para garantir e preservar suas informações de uma gama de novas ameaças.

A partir deste contexto, é possível afirmar que a informação é um ativo valioso para as organizações e, portanto, os ambientes e equipamentos utilizados para processá-la, armazená-la e transmiti-la devem ser protegidos adequadamente (FONTES, 2017).

O Tribunal de Contas da União reforça também a importância da segurança da informação quando, em seu Manual de Boas Práticas em Segurança da Informação, declara:

> Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou concorrentes podem comprometer significativamente não

> apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10).

A norma ABNT NBR ISO/IEC 27002: 2013 reforça a afirmação do autor supracitado, ao declarar que “a informação é um ativo essencial para o negócio de uma organização e necessita ser adequadamente protegida”.

A forma como as organizações geram, processam e disseminam a informação tem se transformado com esses avanços da tecnologia. Acarretando inúmeros paradigmas à segurança da informação, com desafios em assegurar o sigilo, a integridade e a disponibilidade de suas informações (MASCARENHAS NETO; ARAÚJO, 2009).

Atualmente, vivencia-se a guerra cibernética, em que a informação se tornou objeto de desejo das pessoas, e organizações e países buscam incessantemente produzir efeitos maléficos ou benéficos a seus propósitos. Contudo a convergência tecnológica já não possibilita a proibição de alguns recursos tecnológicos dentro do ambiente organizacional, e os mesmos dispositivos e os recursos que podem beneficiar as organizações acabam tornando-as vulneráveis. Um exemplo dessa tecnologia são os dispositivos de *IoT* (MASCARENHAS NETO; ARAÚJO, 2009).

Nesse contexto, a falta da segurança da informação nas organizações as coloca como alvos vulneráveis às mais diversas ameaças.

2.2 Internet das Coisas

O termo Internet das Coisas (*IoT*) foi empregado pela primeira vez como título de uma apresentação que Kevin Ashton fez na *Procter & Gamble* (P&G) em 1999. Ashton integrou o uso de tecnologia de endereçamento de dados com a Internet, seu objetivo era aprimorar o fluxo dos produtos e informações sem a intervenção humana (ASHTON, 2009).

A Internet das Coisas (*IoT*) é um conceito que se refere à conexão inteligente de dispositivos eletrônicos via redes de computadores, permitindo a comunicação e o controle de objetos e processos do mundo real. A *IoT* utiliza a computação para processar dados coletados por sensores e dispositivos inteligentes, a comunicação para transmitir esses dados através de redes, e o controle para automatizar e gerenciar dispositivos e sistemas conectados.

Internet das Coisas (*IoT*) refere-se à interconexão dos objetos físicos do cotidiano à Internet, nos quais muitos desses dispositivos possuem inteligência incorporada e são conectados à rede. Os avanços tecnológicos recentes têm possibilitado a identificação, detecção e controle remoto dessas 'coisas' por meio do uso de sensores e atuadores (FENG; LAURENCE; LIZHE, 2012).

Tem-se como um exemplo de *IoT* a “geladeira do futuro”, que detecta que o leite acabou e o inclui em uma lista de compras para a semana. Entretanto vai muito além disso, é a progressiva automatização de setores inteiros da economia e da vida social tendo como a base a comunicação máquina-máquina: logística, transporte, saúde, produção industrial e muitos outros. Para tal, faz-se fundamental um ambiente favorável ao acesso de um número cada vez com mais dispositivos.

Segundo Magrini (2018, p.20)

> existem fortes divergências em relação ao conceito de *IoT*, não havendo, portando, um conceito único que possa ser considerado pacífico ou unânime. De maneira geral, pode ser entendido como um ambiente de objetes físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia.

O que há em comum entre as definições é que elas se concentram em como computadores, sensores e objetos integarem entre si e processam dados em um contexto de hiperconectividade (MAGRINI, 2018).

A expressão hiperconectividade foi utilizado a principio para caracterizar o estado de disponibilidade dos indivíduos para se comunicar a todo momento. O termo hoje está ligado às comunicações entre indivíduos *(person-to-person, P2P),* indivíduos e máquina *(human-to-machine, H2M)* e entre máquinas *(machine-to-machine, M2M)* atuando, desse modo para diferentes meios de comunicação, tendo nesse cenário um fluxo continuo de informações e intensa produção de dados (MAGRINI, 2018).

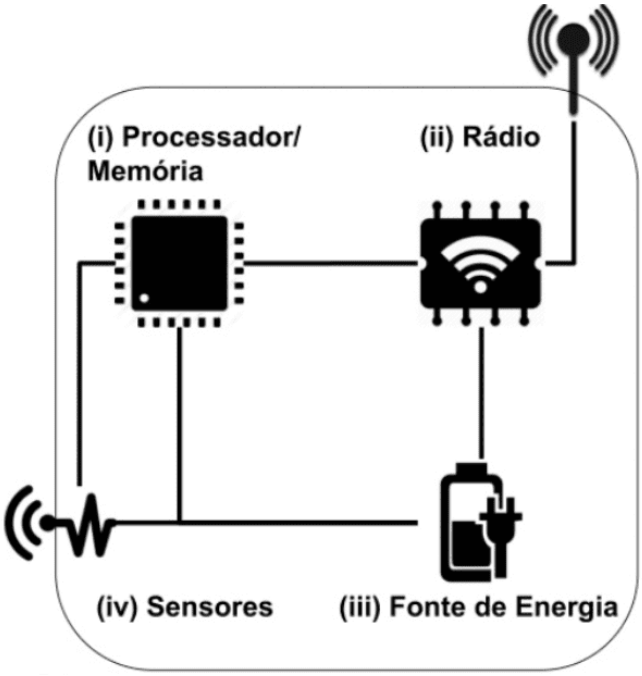
Grande parte dos dispositivos *IoT*, abrangendo câmeras, eletrodomésticos, dispositivos inteligentes ativados por voz, não são arquitetados com a segurança sendo uma prioridade. Com isso, esses equipamentos tornam-se mais suscetíveis, concedendo portas de entrada aos *cibercriminosos.*

Uma exigência necessária para o *IoT* é que seu crescimento não seja realizado causando prejuízo a segurança e a privacidade das pessoas.

2.2.1 Arquitetura de *IoT*

A arquitetura de um dispositivo *IoT* é composta por diferentes componentes que desempenham funções específicas. Segundo Leandro (2019) “os dispositivos *IoT* são compostos basicamente por 4 elementos conforme Figura 1: processador/memória, interface de comunicação, fonte de energia e sensores/atuadores”.

Figura 1: Arquitetura Básica *IoT*



Fonte: Sousa, 2018.

i. Processador/Memória: Essa unidade inclui uma memória interna para armazenamento de dados e programas, um microcontrolador e um conversor analógico-digital para receber sinais dos sensores. Os processadores usados nos dispositivos *IoT* geralmente são os mesmos encontrados em sistemas embarcados e não possuem alta capacidade de processamento. Frequentemente, há também uma memória externa do tipo flash, que serve como memória secundária, por exemplo, para manter um registro de dados. As características desejáveis para essas unidades são baixo consumo de energia e tamanho compacto.

ii. Interface de Comunicação: Essa unidade fornece um canal de comunicação, seja com fio ou sem fio, sendo mais comum o uso de meios sem fio. No caso da comunicação sem fio, a maioria das plataformas utiliza rádios de baixa

potência e custo. Como resultado, a comunicação tem alcance limitado e pode apresentar perdas ocasionais.

iii. Fonte de Energia: Essa unidade é responsável por alimentar os componentes do dispositivo *IoT*. Normalmente, a fonte de energia consiste em uma bateria recarregável ou não, juntamente com um conversor AC/DC. No entanto, existem várias outras fontes de alimentação disponíveis, como energia elétrica e energia solar, entre outras.

iv. Sensores ou Atuadores: Esses elementos têm a função de interagir com o ambiente em que o dispositivo está inserido. Os sensores lidam com grandezas físicas, como temperatura, umidade, pressão, presença, entre outras. Por sua vez, os atuadores são dispositivos que produzem movimento em resposta a comandos, os quais podem ser manuais, elétricos ou mecânicos.

É importante ressaltar que essa descrição apresenta apenas uma visão geral da arquitetura de um dispositivo *IoT* e que podem existir variações e diferentes configurações dependendo da aplicação específica. No entanto, esses componentes básicos fornecem a estrutura fundamental para o funcionamento dos dispositivos *IoT*.

2.3 Aplicações de *IoT*

A Internet das Coisas ajuda a gerenciar e controlar uma variedade de dispositivos e coisas por meio de um método centralizado. Suas aplicações incluem estacionamento inteligente, monitoramento da saúde estrutural, detecção de incêndios florestais, controle da poluição do ar, monitoramento de água potável, sistemas de segurança residencial e alarmes.

Nas cidades inteligentes o conceito envolve a aplicação de tecnologias digitais para melhorar o bem-estar da população, utilizando dados de vários sensores, a *IoT* pode ajudar a resolver problemas como tráfego, gerenciamento de energia, gerenciamento de resíduos, segurança pública, estacionamento inteligente, saúde estrutural, mapas urbanos de ruído, detecção de smartphone etc. (LIMA, 2021).

Tem possibilitado melhor controle do uso de recursos em edifícios e residências, por meio da medição do consumo de energia e água.

A *IoT* está adicionando cada vez mais valor ao setor de saúde, com vantagens significativas que incluem: melhor monitoramento de pacientes, maior eficiência operacional e redução de custos, melhoria na qualidade do atendimento médico, além de possibilitar o desenvolvimento de soluções inovadoras e personalizadas para o cuidado da saúde. Por exemplo o uso durante a pandemia da COVID 19, um sistema chamado *vaccine smart frigde*, que monitora em tempo real o estado e a quantidade das vacinas. Outro exemplo é em relação ao uso de *wearables*, esses dispositivos coletam, armazenam e enviam informações em tempo real sobre o sistema cardiovascular do paciente, detecção de queda etc. (ARAUJO, 2021).

Segundo In Club (2021) “uma solução da IBM utiliza um raciocínio similar ao empregado para acompanhar pacientes com depressão, mas voltado à evolução dos sintomas de *Parkinson*”.

A Internet das Coisas tem se mostrado uma tecnologia útil na detecção de calamidades naturais, de acordo com Sannapureddy (2015). Através do monitoramento das emissões das fábricas e veículos, a *IoT* possibilita a minimização do carbono do ar. Além disso, é possível acompanhar a liberação de produtos químicos nocivos e resíduos nos rios e no mar. A utilização de sensores inteligentes permite monitorar a qualidade da água em rios, lagos e reservatórios, possibilitando a identificação de possíveis fontes de contaminação e alertando sobre a necessidade de ações preventivas para proteger a saúde pública e o meio ambiente. A *IoT* também pode ser usada para enviar alertas de terremotos e tsunamis, detectando tremores, bem como manter o nível de água dos rios e represas sob vigilância, permitindo alertas em caso de inundações.

As aplicações da *IoT* na agricultura são promissoras. De acordo com Liu et al. (2015), a tecnologia tem o potencial de melhorar a segurança e a qualidade dos produtos agrícolas, oferecendo monitoramento contínuo durante todo o ciclo de cultivo. Com sensores inteligentes, é possível monitorar as condições climáticas, do solo e do crescimento das plantas, permitindo que os agricultores tomem decisões mais precisas sobre irrigação, fertilização e colheita. Essa precisão resulta em maior produtividade e qualidade dos cultivos.

Essas são apenas algumas das aplicações de *IoT* que já estão sendo utilizadas em diversos setores. Com o avanço da tecnologia e a evolução das redes de comunicação, é possível que surjam muitas outras soluções inteligentes que nos esperam viver em um mundo mais conectado e eficiente.

2.3.1 Empresas que utilizam *IoT*

A Internet das Coisas está transformando a maneira como as pessoas trabalham. Ela tem aumentado o nível de automatização de processos e a capacidade das análises de dados.

Ao mencionar dispositivos *IoT* deve-se levar em conta a sua separação entre *IoT* doméstico e industrial. Os aparelhos domésticos podem ser desde câmeras, lâmpadas inteligentes até uma assistente virtual. Ao mesmo tempo que os dispositivos industriais têm uma natureza voltada a automatização e coleta de dados através de uma cadeia produtiva da indústria, tal como sensores que captam pressão, umidade e temperatura ou dispositivos elétricos inteligentes que repartem energia de forma eficaz (BERLANDA, 2021).

Se tem alguns outros exemplos dessas utilizações e aplicações industriais, uma delas é a plataforma da Newatt utiliza o *machine learning*, através dele a máquina reconhece padrões conseguindo comunicar sobre desperdícios de energia, enviando alertas por meio do aplicativo (ALPER SEGUROS, 2020).

Uma outra aplicação é no setor da agricultura a Agrosmart está desenvolvendo uma ferramenta que ao se conectar com uma armadilha de pragas, vai ajudar o produtor a aplicar o defensivo agrícola no momento correto e na quantidade ideal, para alcançar maior eficácia no combate às pragas, com custo reduzido e diminuindo o impacto ambiental, os sensores estando conectados aos sistemas, irão realizar a coleta dos dados, enviando para a internet, onde será realizado o processamento das imagens, a contagem e identificação das pragas, essas informações chegaram ao produtor por meio de um *tablet*, um *smartphone* ou outros dispositivos semelhantes (ALPER SEGUROS, 2020).

A empresa de logística alemã DHL implementou o recurso com o intuito de agilizar a administração de pátios para a logística de entrada para fabricação. Também implementou cockpits de *IoT* em três de seus armazéns inteligentes na Alemanha, Holanda e Polônia. Isso permitiu que a DHL monitorasse as atividades em tempo real (COMPUTERWORLD UK, 2019).

A empresa Konux entrega soluções de *IoT* que permitem a manutenção preditiva às empresas ferroviárias e industriais utilizando uma combinação de

sensores inteligentes e análises baseadas em inteligência artificial. As empresas então são fornecidas com uma visão clara e em tempo real sobre a integridade de suas máquinas (COMPUTERWORLD UK, 2019).

2.4 Desafios dos Dispositivos *IoT* para a Segurança da Informação

A Internet das Coisas (*IoT*) é um mercado em rápida expansão que traz consigo uma série de desafios significativos para a segurança da informação. Embora a conexão, autenticação e segurança na comunicação de dispositivos *IoT* seja uma obrigação, muitas vezes, as soluções disponíveis não são adequadas para garantir a proteção adequada.

Um dos desafios mais críticos é a questão dos dispositivos *IoT* não confiáveis com acesso. O aumento exponencial e acelerado do número desses aparelhos no mercado corrobora o fato de que muitos são fabricados por empresas com diferentes padrões de segurança, sendo que numerosos fabricantes ainda não estão familiarizados com as boras práticas de Segurança da Informação. Nesse sentido, muitos dispositivos *IoT* não possuem medidas de segurança em rede coordenadas, não exigem senhas ou não se preocupam com a complexidade delas. Além disso, eles frequentemente armazenam informações pessoais e apresentam diversas vulnerabilidades (ZANI, 2016).

Como resultado, os dispositivos não confiáveis podem ser vulneráveis a ataques cibernéticos, o que pode levar a violações de segurança graves e potencialmente dispendiosas.

Além disso, outro problema relacionado aos dispositivos *IoT* é a questão dos ataques de força bruta na infraestrutura *IoT*. Nesse tipo de ataque, o objetivo é obter um conjunto de todas as combinações possíveis de senhas para quebrar a criptografia de uma senha. O alvo mais comum são os arquivos de senhas em texto simples que são criptografados, como, por exemplo, o arquivo de senhas dos usuários do sistema operacional Linux (RAZA et al., 2012)

Em uma infraestrutura *IoT*, esses ataques podem ser particularmente prejudiciais, pois os dispositivos *IoT* com poucas opções de segurança e vulneráveis a ataques devido à falta de atualizações ou patches de segurança, podem ser usados em sistemas críticos, como sistemas de controle de energia ou sistemas de controle de tráfego, e um ataque bem-sucedido pode ter consequências graves.

2.4.1 Desafios dos dispositivos *IoT*

Um dos principais desafios é a necessidade de criptografar dados sensíveis que podem ser facilmente interceptados por terceiros mal-intencionados. Os dispositivos *IoT* muitas vezes usam protocolos de comunicação sem fio para se comunicar com outros dispositivos.

Os protocolos de comunicação sem fio geralmente transmitem dados em texto claro, possibilitando que qualquer pessoa que esteja interceptando a transmissão leia os dados. Essa condição é especialmente problemática quando os dados transmitidos contêm informações sensíveis, como senhas, chaves criptográficas ou informações pessoais.

Para proteger esses dados, é necessário que a criptografia seja aplicada adequadamente, o que aponta para um novo desafio: O aumento significativo das demandas de energia e recursos do dispositivo.

Devido à limitação de poder computacional da maioria dos dispositivos *IoT*, podem surgir desafios na implementação de medidas de segurança, como criptografia, senhas e o uso de algoritmos mais avançados (Leandro Rogério Corrêa Leite, 2019). A implementação de algoritmos de criptografia pesados e complexos pode exigir muitos recursos do sistema host, afetando o desempenho do dispositivo e levando a problemas como atrasos na resposta, consumo excessivo de energia ou até mesmo falhas no sistema.

O endereçamento em dispositivos *IoT* é um desafio crítico que apresenta dois problemas principais: A compatibilidade com o endereçamento existente e a indisponibilidade de mais endereços IPV4.

Muitos equipamentos foram projetados para se comunicar com outros dispositivos *IoT*, utilizando protocolos e endereços diferentes dos dispositivos convencionais na rede. Isso pode criar implicações de interoperabilidade e dificultar a comunicação entre os dispositivos *IoT* e outros aparelhos conectados à rede.

Além disso, o crescente número de dispositivos *IoT* sendo adicionados às redes propicia o desafio em manter um endereçamento único e gerenciável para cada dispositivo.

O protocolo IPv4, amplamente utilizado em redes de computadores, apresenta previsibilidade de indisponibilidade de endereços ao passo que o elevado número de dispositivos *IoT* se conecta à rede.

Nesse sentido, já se iniciou a utilização no protocolo IPV6 como a grande solução para o enfrentamento desse desafio. Este novo protocolo atenderá a escassez de endereçamento do IPv4 e marcará o advento da era da "Internet das Coisas". Com esse protocolo, teremos a capacidade de conectar todos os dispositivos eletrônicos, sem preocupações com limites de endereços IP, pois haverá disponibilidade para qualquer dispositivo que precise estar conectado à internet (CLEISON, 2017).

O grande volume de dados gerados pelos dispositivos *IoT* apresenta desafios significativos ao universo da computação.

Há uma grande dificuldade em manter largura de banda suficiente para atender à demanda de dados gerados por esses dispositivos, visto que o tráfego de dados pode aumentar exponencialmente, sobrecarregando a infraestrutura de computação e causar congestionamentos e falhas. Isso pode ser especialmente problemático em redes de computadores com recursos limitados, como redes sem fio e dispositivos móveis.

Tal cenário torna difícil o fornecimento de serviços eficientes e confiáveis, como análise em tempo real, processamento de dados e armazenamento em nuvem.

Outro desafio importante se refere à análise de tráfego. Os dispositivos *IoT* geram uma quantidade significativa de dados que podem ser usados para monitorar e controlar dispositivos, coletar informações para análise e fornecer feedback aos usuários. No entanto, a análise de tráfego pode ser difícil em grandes volumes de dados. Nesse sentido, os dispositivos *IoT* podem ser alvos vulneráveis para ataques de *hackers* e cibercriminosos, o que pode levar a vazamentos de dados ou outras violações de segurança.

2.5 Riscos decorrentes da utilização de *IoT*

Cada um dos inúmeros dispositivos *IoT* existentes nas casas e empresas são um eventual ponto de vulnerabilidade e estes equipamentos conectados podem ser utilizados como uma forma de entrada para a rede, podendo assim ser um ponto de início de um grande ataque.

Todos os aparelhos estão interconectados no cenário de *IoT*, tem-se então diversos problemas que podem ser decorrentes, pois se um único dispositivo estiver mal protegido e conectado à rede, ele pode por consequência afetar toda a segurança da rede (FIGUEIRA, 2016).

Estes dispositivos apresentam uma característica que acaba contribuindo para a ocorrência do problema anterior, diversos tipos destes equipamentos são implementados em massa, por exemplo, o caso dos sensores, o que aumenta a chance de algum deles estar desprotegido. Além do mais, outros problemas podem ser gerados a partir das particularidades da *IoT*, nela as comunicações podem ser realizadas por meio de redes sem fio, que podem ser colocados em locais públicos estando assim ao alcance de qualquer indivíduo, a demais muitos dispositivos possuem recursos limitados, onde medida de segurança que demandam processamento poderiam acarretar impactos como redução das funcionalidades do dispositivo (FIGUEIRA, 2016).

Em uma pesquisa apresentada em 2019, foi descoberto que 91,5% das transações de dados realizadas por dispositivos *IoT* em redes corporativas não são criptografadas, tornando-as suscetíveis a variados tipos de ataques (BERLANDA, 2021).

Segundo (BERLANDA, 2021), isso ocorre, pois os dispositivos *IoT* ficam em grande parte localizados nas extremidades da rede, e fisicamente em locais de fácil acesso para qualquer pessoa mal-intencionada.

Com a entrada em vigor da Lei Geral de Proteção do Dados Pessoais (LGPD) em 2020 esses cuidados com a segurança dos dados devem que ter ainda mais importância. Com esta lei, todas as empresas que realizam tratamento de dados pessoais devem aderir uma série de medidas para garantir o cumprimento da legislação, de modo que a privacidade, transparência, desenvolvimento, padronização, proteção do mercado e a concorrência sejam asseguradas (MACHADO MEYER SENDACZ OPICE ADVOGADOS, 2018).

De acordo com Menezes (2017),

> o Brasil está entre um dos países mais atacados pela *botnet* Mirai, que contamina câmeras de segurança IP, gravadores digitais de vídeo (DVRs) e outros dispositivos de Internet das Coisas, como impressoras e roteadores.

Os *botnets* baseiam-se no conceito de diversos dispositivos infectados, conectados à internet, que permitem com que o hacker possa realizar ataques de

negação de serviço distribuída (conhecido como *DDos - Distributed Denial-of-Service attack* - em inglês). O *botnet Mirai* é um malware que infecta dispositivos inteligentes que rodam em processadores ARC, transformando-os em uma rede de *bots* controlados remotamente (BERLANDA, 2021).

Diante desses cenários, pessoas com más intenções podem utilizar essas vulnerabilidades para realizar inúmeros tipos de ataques, como *man-in-the-middle, DDoS, sniffing* entre outros, Estes ataques podem ter como objetivo apenas a captura dos dados que correm na rede, a alteração deles ou até mesmo deixar a rede fora do ar.

2.5.1 Principais Tipos de Ataques em Dispositivos *IoT*

À medida que a conectividade se expande, a possibilidade de enfrentar ataques cibernéticos também aumenta. Nesse contexto, é crucial entender que qualquer dispositivo conectado à internet está suscetível a ataques em algum momento. Os invasores empregam métodos diferentes, desde o roubo de credenciais à exploração de vulnerabilidades, até tentar comprometer remotamente os dispositivos de *IoT*. Uma vez que obtêm controle sobre um dispositivo de *IoT*, os invasores podem utilizar essa posição para roubar dados, executar ataques de negação de serviço distribuído (*DDoS*) ou até mesmo tentar comprometer o restante da rede conectada.

Ataques de Controle: Os invasores visam assumir o controle dos dispositivos *IoT* para obter acesso não autorizado e manipular suas funcionalidades. Eles exploram vulnerabilidades ou utilizam técnicas como injeção de comandos para assumir o controle. Um exemplo notável é o ataque à rede elétrica ucraniana em 2015, em que hackers assumiram a manipulação dos sistemas de controle industrial através de dispositivos de *IoT*, causando um apagão em larga escala (ZETTER, 2016).

Ataques de Roubo de Informações: Os invasores direcionam dispositivos *IoT* para obter informações confidenciais, como dados pessoais, informações de saúde e senhas armazenadas nos dispositivos. Eles exploram vulnerabilidades ou interceptam comunicações para acessar essas informações. Um exemplo é o ataque ao sistema de monitoramento de câmeras da *Verkada*, em que invasores conseguiram acesso a *feeds* de vídeo de câmeras de segurança (SONNEMAKER, 2021).

Ataques de Interrupção de Serviços: Os ataques de negação de serviço distribuído (*DDoS*) são comuns em dispositivos *IoT*. Os invasores utilizam uma rede

de dispositivos comprometidos, formando uma *botnet*, para inundar o sistema-alvo com tráfego excessivo, tornando-o inacessível para os usuários legítimos. Um exemplo é o ataque Dyn em 2016. Nesse caso, uma *botnet* composta por dispositivos *IoT* infectados foi utilizada para realizar um ataque *DDoS* em larga escala contra os servidores DNS da Dyn, resultando em interrupções significativas nos serviços online, afetando empresas como Twitter, Spotify e Reddit (KREBS, 2016). Esse incidente destacou a vulnerabilidade dos dispositivos *IoT* e a capacidade de causar interrupções em serviços essenciais na internet. Além disso, o ataque *BrickerBot* também ocorrido em 2016, tinha como objetivo inutilizar permanentemente os dispositivos *IoT*, explorando vulnerabilidades conhecidas e corrompendo seus sistemas (GOODIN, 2017).

3 DESENVOLVIMENTO

A segurança em sistemas *IoT* tem se tornado uma preocupação crescente devido ao avanço rápido da tecnologia e à frente de dispositivos interconectados. Este trabalho tem como objetivo explorar a segurança em *IoT* por meio de uma prática desenvolvida no simulador PICSimLab. Serão examinados três aspectos-chave da segurança: ataques de controle, intercepção de informação e interrupção de serviço.

De forma resumida, o PicSimLab é um ambiente de simulação de circuitos eletrônicos baseado no microcontrolador PIC. Ele permite simular o comportamento de circuitos eletrônicos que utilizam microcontroladores PIC, como projetos de automação residencial, sistemas de controle, sensores, entre outros.

O PicSimLab oferece uma interface gráfica intuitiva onde os usuários podem projetar e simular circuitos eletrônicos complexos. Ele inclui recursos como uma biblioteca de componentes eletrônicos, um editor de código-fonte para programação em linguagem C, suporte para depuração passo a passo e uma variedade de ferramentas de análise de circuitos.

Nesse sentido, a metodologia adotada para alcançar os objetivos propostos envolveu diversas etapas:

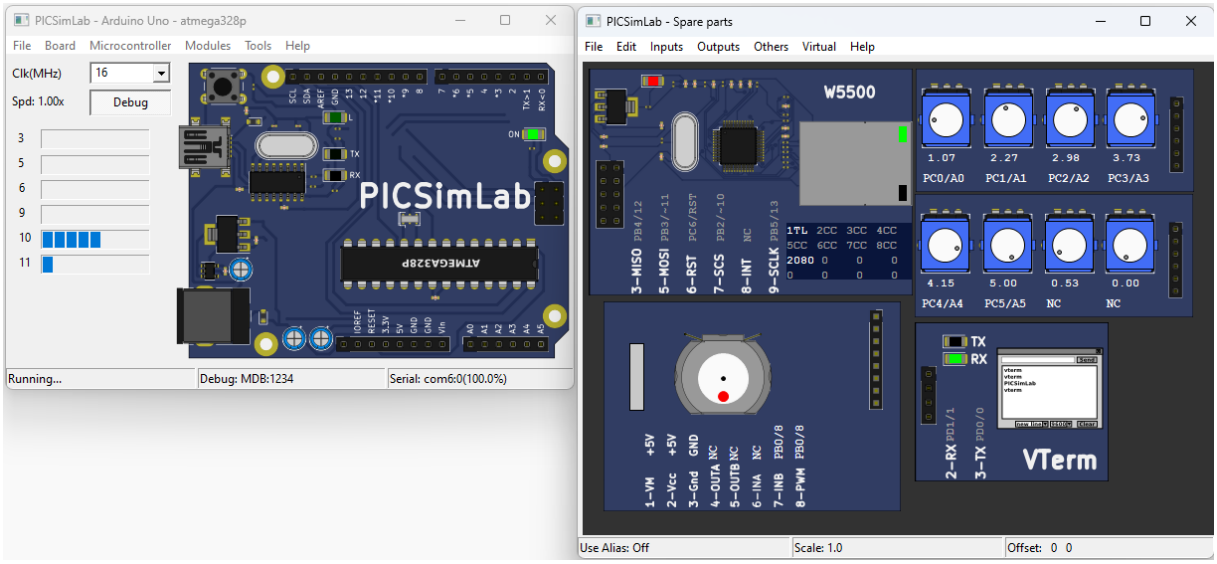
Configuração do ambiente: Instalamos e configuramos o PICSimLab, como base para a implementação do sistema *IoT* simulado.

Projeto do sistema *IoT*: Definimos o escopo do sistema *IoT* simulado, identificando os dispositivos envolvidos, como sensores, atuadores e microcontroladores PIC. Além disso, elaboramos uma arquitetura de rede que permite uma comunicação entre esses dispositivos.

Com a estrutura definida, partimos para a implementação da comunicação entre os dispositivos utilizando as bibliotecas e recursos disponíveis no PICSimLab. Essa etapa foi fundamental para simular a interação e troca de dados entre os componentes do sistema.

Apresentaremos algumas imagens que ilustram o desenvolvimento do projeto. A Figura 2 mostra o protótipo do circuito implementado no PICSimLab, proporcionando uma representação visual do sistema *IoT* simulado. Em seguida, temos a Figura 3, que descreve os campos de retorno do objeto, oferecendo informações sobre os dados coletados pelos sensores.

Figura 2: Protótipo do Circuito



Fonte: PicSimLab.

Figura 3: Descrição dos campos de retorno do objeto

Fonte: Elaborado pelo autor, 2023.

Já as Figuras 4 e 5 demonstram a ativação e desativação do motor, exemplificando a capacidade de controle do sistema sobre os atuadores. Essas imagens foram elaboradas pelo autor como parte do processo de implementação e teste do sistema.

Figura 4: Ativação do motor

Fonte: Elaborado pelo autor, 2023.

Figura 5: Desativação do motor

Fonte: Elaborado pelo autor, 2023.

Dando continuidade, focamos nos três aspectos-chave da segurança em IoT. No que diz respeito aos ataques de controle, identificamos possíveis vulnerabilidades no sistema IoT simulado e implementamos ataques controlados. Exploramos falhas de segurança conhecidas ou injetamos comandos maliciosos para alterar o comportamento normal dos dispositivos.

Quanto à intercepção de informação, desenvolvemos um sniffer de rede para capturar e analisar pacotes de dados trocados entre os dispositivos. Identificamos informações transmitidas ou padrões de comunicação que poderiam ser explorados por um atacante.

Por fim, abordamos a interrupção de serviço, simulando a ocorrência de ataques de negação de serviço no sistema IoT simulado. Ao enviar uma quantidade

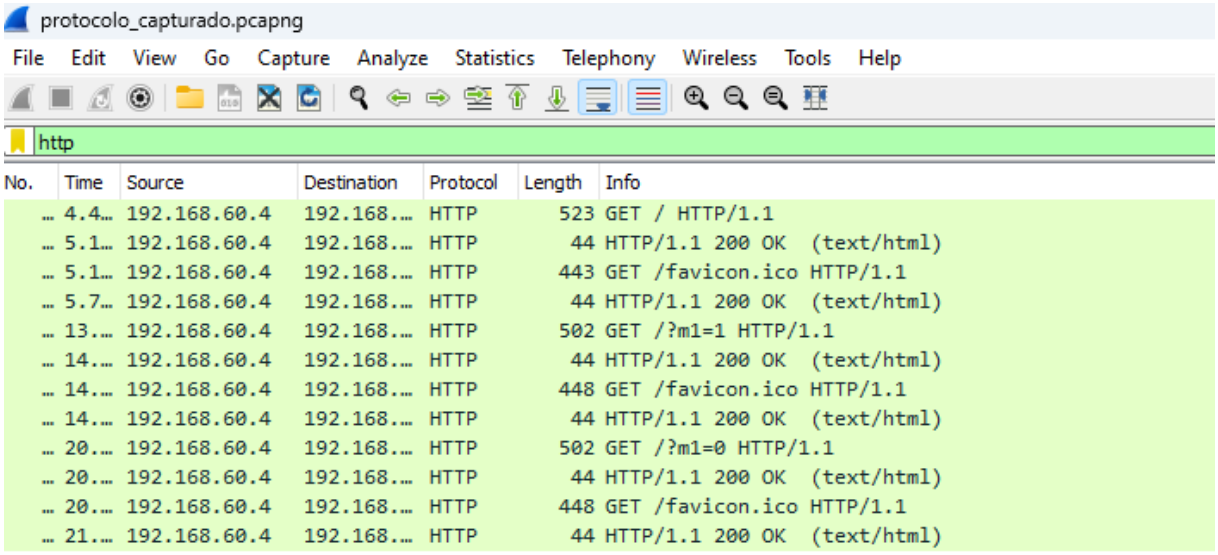
excessiva de requisições de comunicação, demonstramos como o sistema pode ser afetado e tornar-se indisponível.

I. Realização de testes

i. Intercepção de informação

Utilizamos o Wireshark para capturar e analisar pacotes de dados trocados entre os dispositivos. Realizamos a captura de pacotes por meio da configuração de captura "*adapter for loopback traffic*" no Wireshark, com um filtro aplicado para capturar apenas o tráfego relacionado ao protocolo HTTP conforme Figura 6.

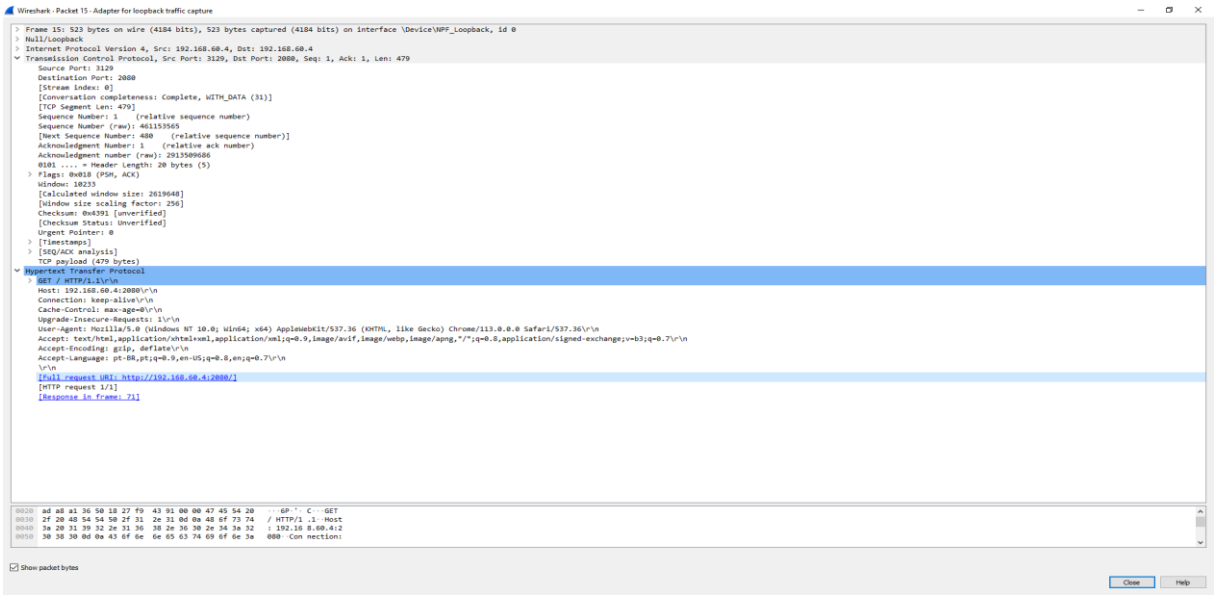
Figura 6: Pacotes capturados.



Fonte: Wireshark,1998-2023.

Através dessa captura, obtivemos pacotes que representavam diferentes estados e ações no sistema, como o status inicial demonstrado na Figura 7, ativação e desativação do motor.

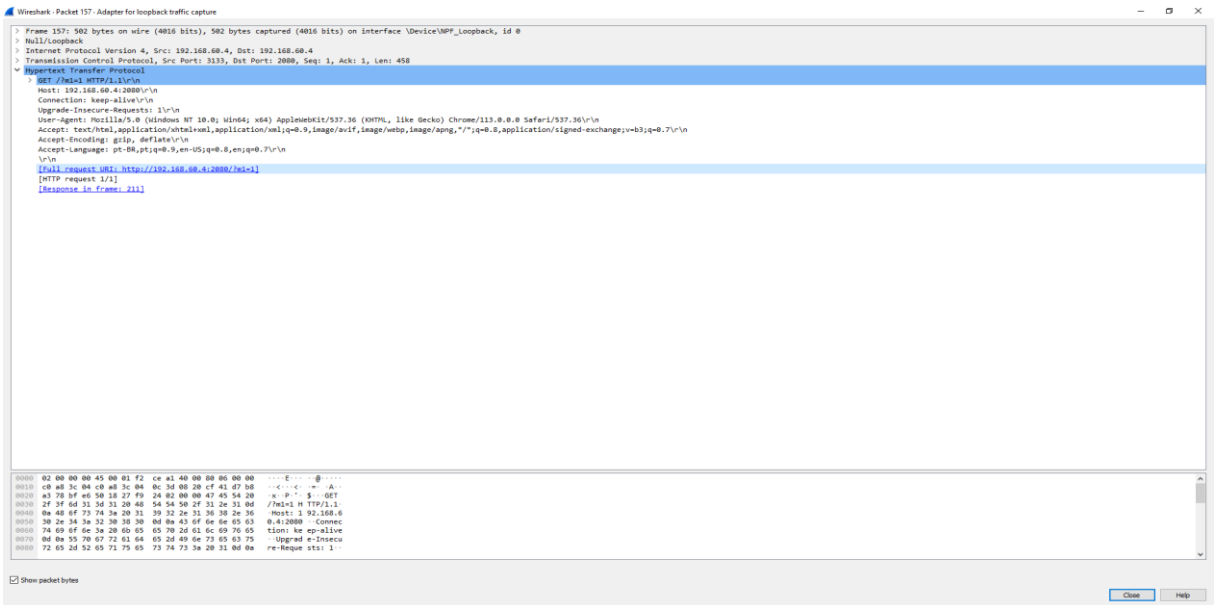
Figura 7: Captura status inicial.



Fonte: Wireshark, 1998-2023.

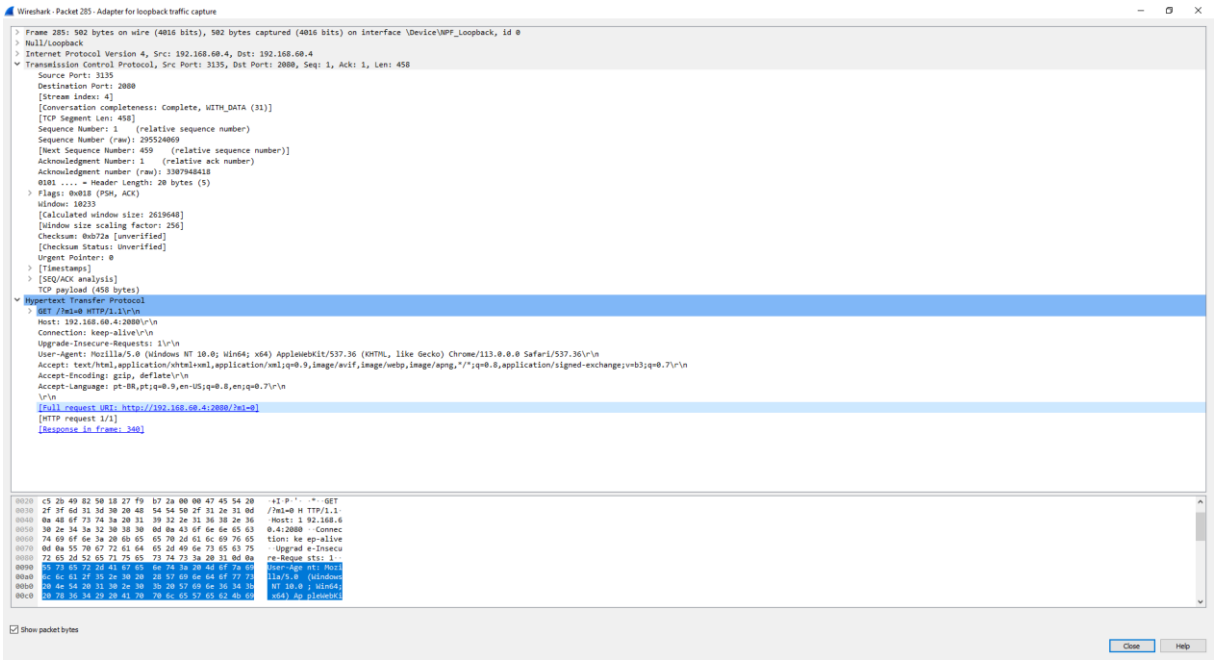
Esses pacotes continham informações detalhadas sobre os comandos utilizados para executar essas ações específicas. Por exemplo, o comando de ativação era representado pelo valor "m1=1" conforme Figura 8, enquanto o comando de desativação era representado por "m1=0" conforme Figura 9.

Figura 8: Captura ativando o motor.



Fonte: Wireshark, 1998-2023.

Figura 9: Captura desativando o motor.



Fonte: Wireshark, 1998-2023.

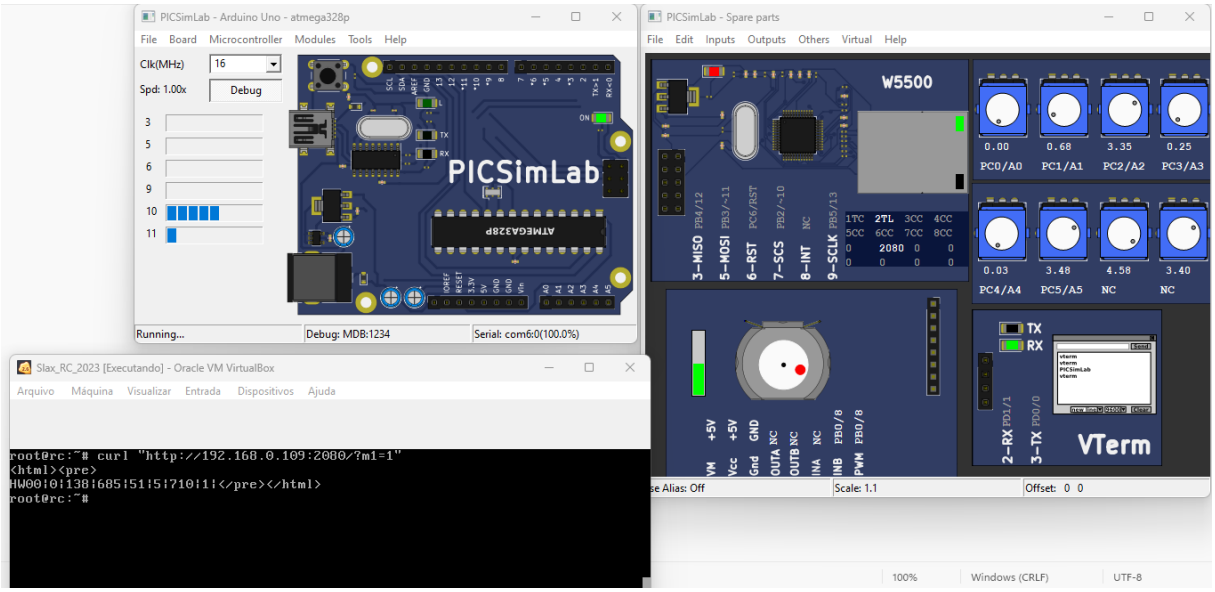
Ao analisar os pacotes capturados, pudemos compreender melhor como os comandos são transmitidos e interpretados pelo sistema, contribuindo para um melhor entendimento das operações realizadas e das interações entre os dispositivos envolvidos no projeto.

ii. Ataques de controle

Com base nas informações capturadas, foi realizado um teste utilizando uma máquina virtual Linux com o objetivo de controlar um serviço específico, mais precisamente o motor. O propósito desse teste era verificar a capacidade de enviar comandos de ativação e desativação para o motor.

O teste foi conduzido através da execução do seguinte comando:

Figura 10: Comando de ativação do motor.



Fonte: VM VirtualBox, 2021; PicSimLab, 2023.

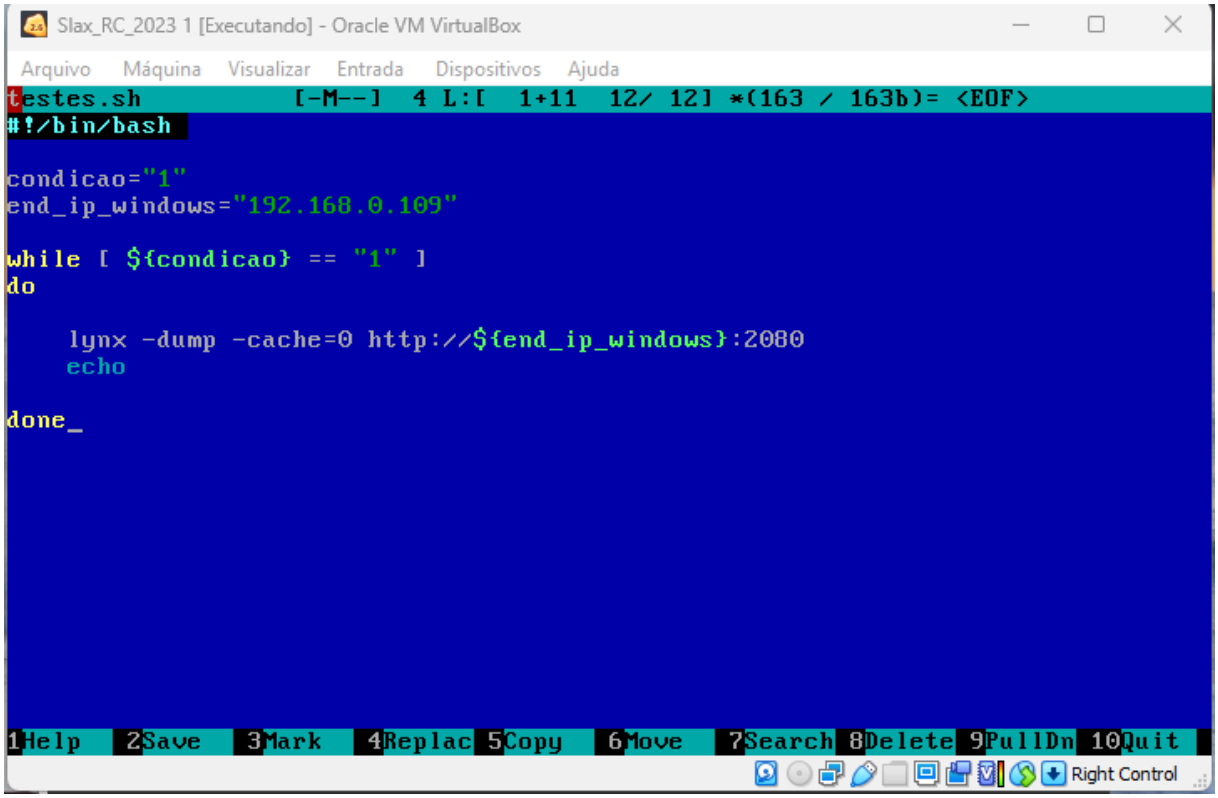
Esse comando utiliza o utilitário *curl* para enviar uma solicitação *GET* para o endereço IP especificado, com o parâmetro m1 definido como 1, indicando o comando de ativação do motor sem autenticação adequada.

Como resultado do teste, foi possível ligar o motor demonstrado na Figura 10, uma vez que o servidor do serviço interpretou a solicitação recebida e executou o comando de ativação correspondente.

iii. Interrupção de serviço

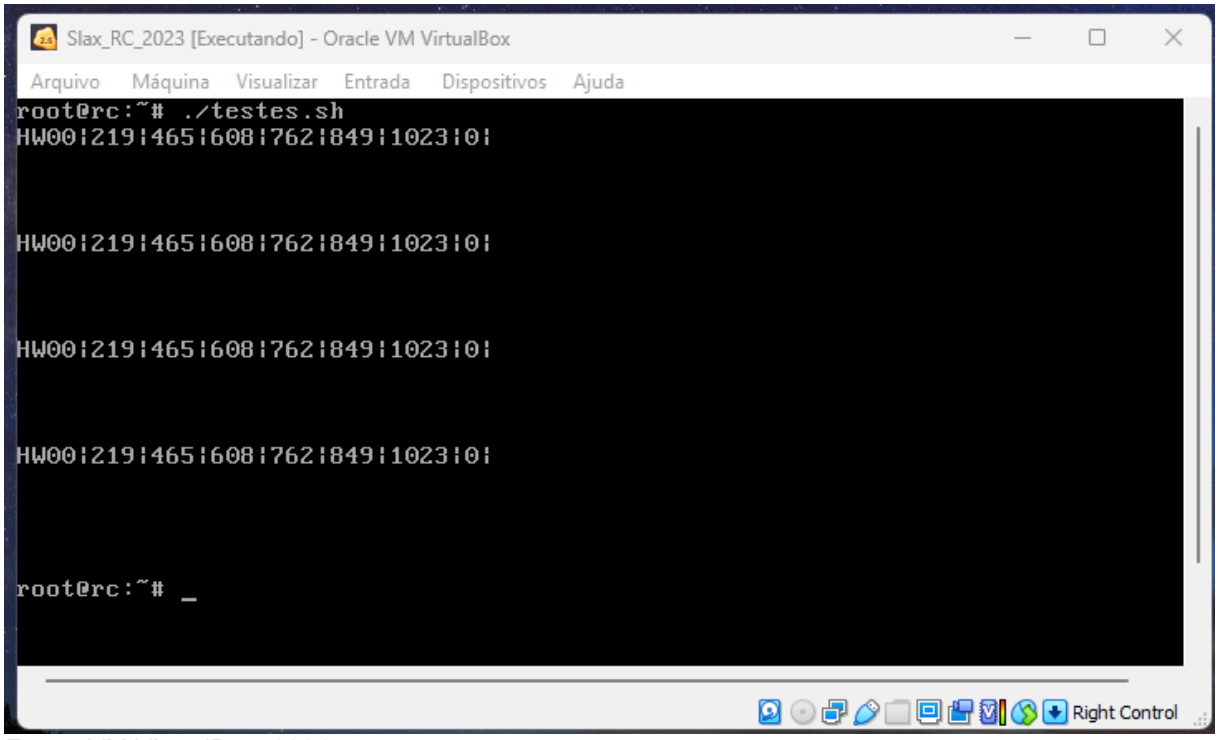
A interrupção de serviço foi realizada por meio de um *script* em *Bash* conforme Figura 11, que cria um *loop* infinito para executar repetidamente uma solicitação HTTP em várias máquinas virtuais (VMs). O objetivo desse teste era causar a interrupção do serviço, impossibilitando a comunicação, porém mesmo com as seis VMs em execução, a comunicação ainda era possível.

Figura 11: *Script* em *Bash* que cria um *loop* infinito para executar repetidamente solicitação HTTP.



Fonte: VM VirtualBox, 2021.

Figura 12: Execução do *script*.

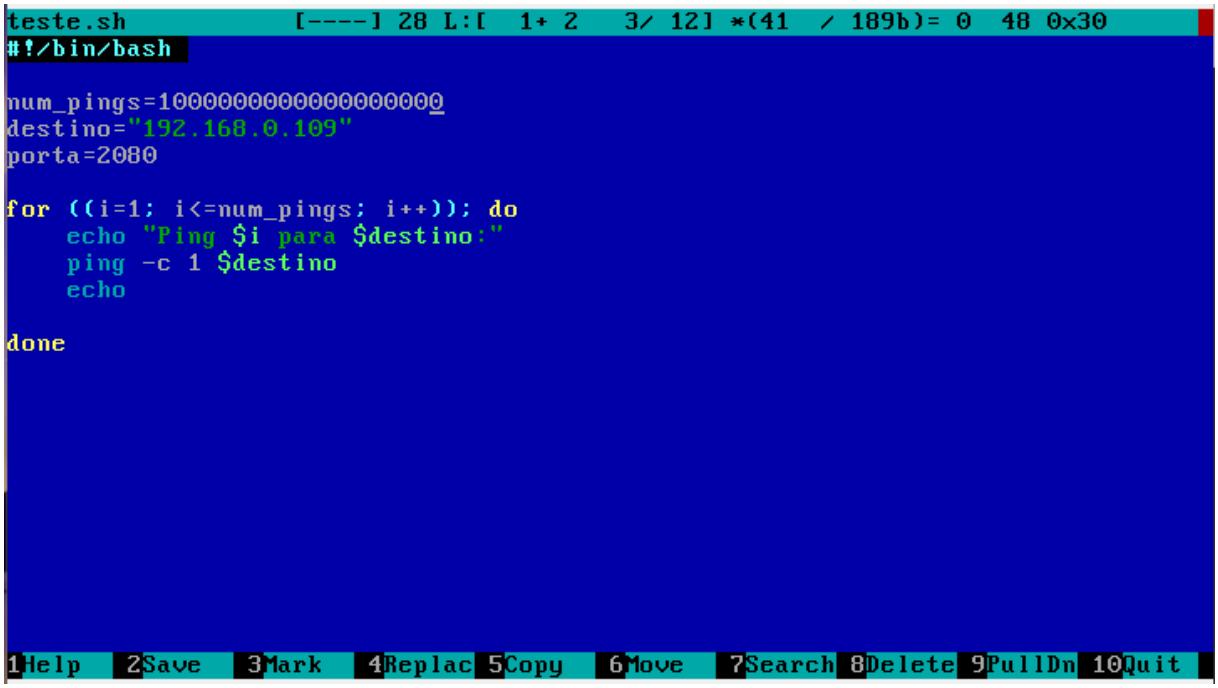


Fonte: VM VirtualBox, 2021.

Adicionalmente, realizamos outro teste utilizando cinco máquinas virtuais Linux, onde um *script* foi utilizado para enviar *pings* e congestionar o serviço. O objetivo era simular um cenário de falha no qual o motor não pudesse receber comandos de ativação e desativação. Como resultado, ao tentar acessar o projeto através do navegador, os usuários recebiam uma mensagem informando que a conexão foi recusada.

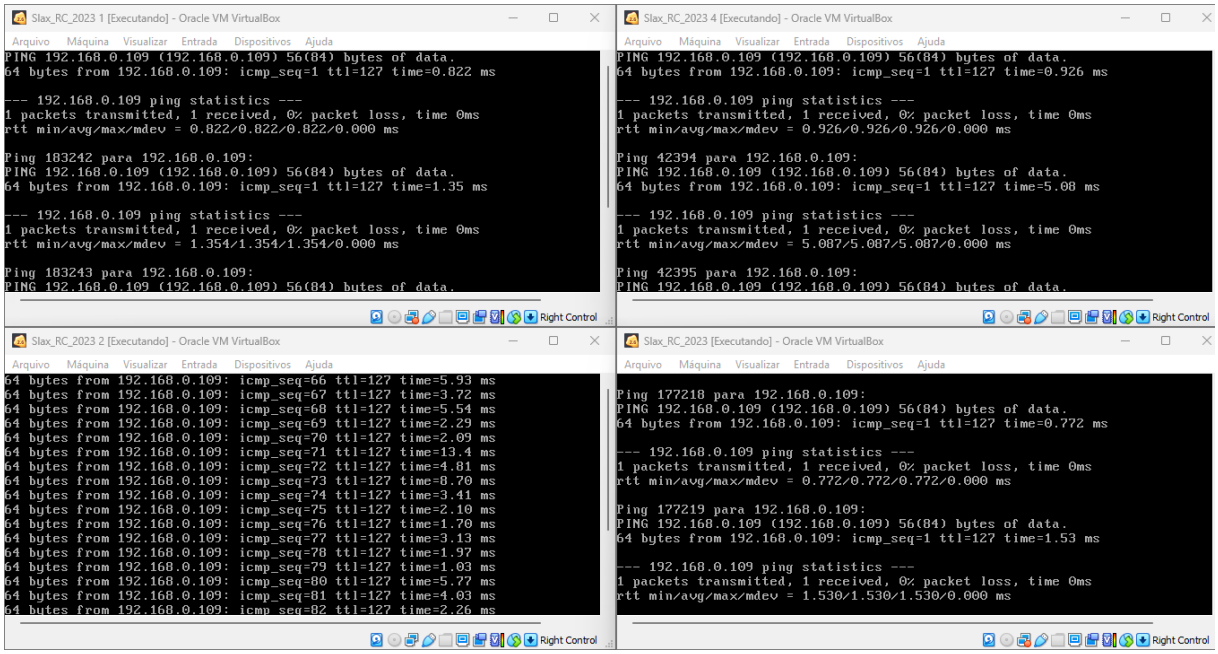
O teste foi executado através de um *script* em *shell* conforme Figura 13, que utilizava o comando de *ping* para enviar um número determinado de *pings* para o endereço IP do serviço ou máquina-alvo. O número de *pings* enviados era controlado pela variável "*num_pings*", enquanto a variável "destino" definia o endereço IP do alvo do teste. A porta pela qual o serviço estava disponível era indicada pela variável "porta". O *script* implementava um *loop* para enviar os *pings* repetidamente, exibindo uma mensagem com o número do *ping* e o destino a cada iteração.

Figura 13: *Script* em *shell.*



Fonte: VM VirtualBox, 2021.

Figura 14: *Script* em execução.



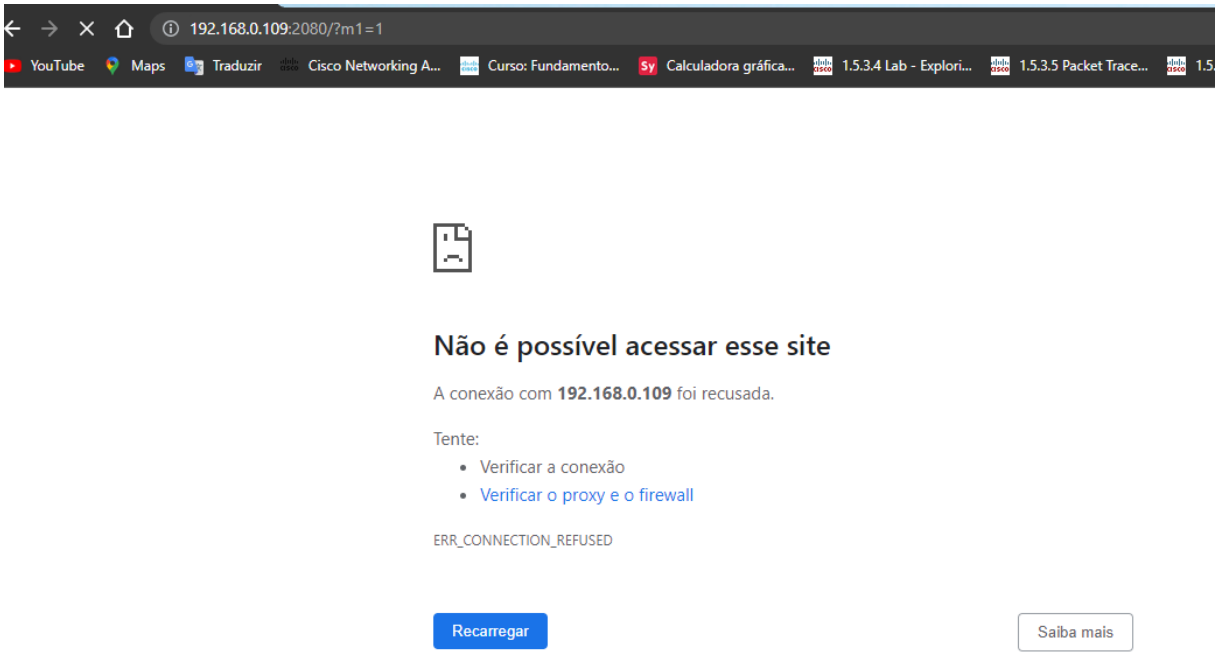
Fonte: VM VirtualBox, 2021.

Os resultados desse teste demonstraram que a interrupção da comunicação, foi bem-sucedida, pois a conexão com o motor foi recusada conforme Figura 16, impossibilitando o envio de comandos de ativação e desativação.

Figura 15: Interrupção da ativação do motor.

Fonte: Elaborado pelo autor, 2023.

Figura 16: Conexão recusada.



Fonte: Elaborado pelo autor, 2023.

4 RESULTADO E DISCUSSÃO

Analisamos os resultados obtidos ao explorar as vulnerabilidades e realizamos uma avaliação dos riscos e riscos identificados. Discutimos possíveis medidas de segurança e recomendações para mitigar essas ameaças em um ambiente real. Tais recomendações se baseiam em alguns pontos cruciais que a Segurança da Informação considera para possibilitar a segurança dos dispositivos *IoT*:

Criptografia: É essencial a utilização de algoritmos de criptografia robustos para proteger a transmissão de dados, implementar protocolos seguros de autenticação e gerenciamento de chaves para garantir que apenas dispositivos autorizados possam acessar os dados. É importante considerar a implementação de hardware dedicado para criptografia, em vez de depender exclusivamente do processamento do sistema host.

Uma solução popular para a criptografia em dispositivos *IoT* é a criptografia de chave simétrica de baixa potência, que usa algoritmos de criptografia leves e eficientes em termos de energia. Além disso, a criptografia de chave pública também pode ser implementada de forma eficaz em dispositivos *IoT*, desde que seja usada com moderação e com o tamanho de chave apropriado para o dispositivo.

De modo geral, é fundamental que os fabricantes de dispositivos *IoT* e as empresas que os utilizam implementem soluções de criptografia eficazes, mas conscientes dos recursos. Os especialistas em segurança da informação devem trabalhar em conjunto com os fabricantes de dispositivos *IoT* para garantir que os dispositivos sejam seguros e protejam os dados sensíveis dos usuários.

Utilização de tecnologias atuais e inteligentes: Para se combater novas ameaças, é preciso utilizar as novas tecnologias do mercado. Nesse sentido, a integração de firewalls de rede (como recursos de antivírus e antispam) com a tecnologias da computação em nuvem distribuída pode se apresentar como uma das soluções possíveis para superar esses desafios.

A implantação de recursos de computação em nuvem distribuída pode reduzir a latência e melhorar o desempenho da rede de modo a garantir que a largura de banda seja suficiente para atender à demanda de dados gerados por esses dispositivos. Além disso, muitas soluções em nuvem possibilitam a análise de dados em tempo real, um recurso fundamental para detectar ameaças de segurança nos dispositivos *IoT* através da monitoração e análise do tráfego de dados.

Para os ataques de controle, além da utilização de firewalls, é importante o investimento em tecnologias que garantam a segurança dos controles de acesso. A computação em nuvem também oferece serviços para essa demanda, como o IAM Management da AWS, RBAC do Azure ou o IAM GCP. No entanto, independentemente da utilização da nuvem ou não, é imprescindível a utilização de Multifator de Autenticação (MFA) para o acesso aos dispositivos IoT. A boa prática contempla o requerimento de senhas, biometria, algum objeto ou mesmo reconhecimento facial para a permissão de acesso.

CONSIDERAÇÕES FINAIS

Mediante o exposto, precisamos retornar ao contexto inicial de que, atualmente, há um notável crescimento de dispositivos *IoT*, de modo que estes apresentam grande relevância para diversos modelos de negócios e fazem parte da cadência cotidiana da maior parte dos indivíduos.

Nesse sentido, considerando os diversos desafios na área de segurança, privacidade e integridade, foi proposta a seguinte reflexão como problema de pesquisa deste projeto: Como melhorar a performance de segurança de dados e informações, em dispositivos *IoT*?

Para responder a essa questão, foi necessário entender o funcionamento de um dispositivo *IoT*, a sua composição, discernir sobre as principais vulnerabilidades em que estes aparelhos estão expostos e a influência das boas práticas de Segurança da Informação, exercidas pelos seres humanos, desde a fabricação dos dispositivos.

Assim, com o objetivo de demonstrar de maneira macro a fragilidade de segurança em muitos destes dispositivos, realizamos com sucesso três tipos de ataques a um exemplar de aparelho *IoT* em PicSimLab, evidenciando a possibilidade de roubar informações, assumir o controle e mesmo interromper o funcionamento do aparelho.

Em vista disso, para enfrentar os desafios que os dispositivos *IoT* proporcionam à Segurança da Informação, é necessário aos fabricantes destes aparelhos e as empresas que os utilizam adotarem uma abordagem proativa de segurança da informação. Isso inclui a implementação de protocolos de segurança adequados, a atualização regular dos dispositivos e a monitoração constante de vulnerabilidades e ameaças potenciais.

Além disso, as empresas também devem investir em programas de treinamento de conscientização de segurança para garantir que seus funcionários estejam cientes dos riscos de segurança associados aos dispositivos *IoT* e saibam como se proteger contra eles.

Por fim, é importante ressaltar que a segurança em dispositivos *IoT* é um desafio em constante evolução. À medida que a tecnologia avança e novas ameaças surgem, é necessário um compromisso contínuo com a pesquisa, inovação e atualização das medidas de segurança.

REFERÊNCIAS

ALPER SEGUROS. **Internet das coisas: como as grandes empresas usam *IoT*.** 2020. Disponível em: https://www.alperseguros.com.br/internet-das-coisas/ Acesso em: 22 nov. 2022.

ASHTON, Kevin. ***That 'Internet of Things' thing*.** Publicado no RFID Journal, 2009. Disponível em: https://www.rfidjournal.com/that-internet-of-things-thing Acesso em: 24 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002: Tecnologia da Informação, técnicas de segurança e código de prática para controles de segurança da informação**. Rio de janeiro, 2013. Disponível em: https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf Acesso em: 22 nov. 2022.

ARAUJO, Diogo Raposo Bastos. "***IOT* na saúde: entenda sua importância e como utilizá-lo**. 17 de dezembro de 2021 Disponível em: https://blog.jaleko.com.br/*IoT*-na-saude/ Acesso em: 01 maio 2023.

BERLANDA, Rodrigo Grando. **Guia de segurança da informação para a conectividade de dispositivos *IoT*.** Trabalho de Conclusão de Curso - Instituto Federal de Santa Catarina, 2021. Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/2304/CSTGTI%20-%20TCC%20-%20Rodrigo%20Grando%20Berlanda%20-%20Guia%20de%20seguranca%20da%20informacao%20para%20a%20conectividade%20de%20dispositivos%20IoT%20-%20Assinado.pdf?sequence=1 Acesso em: 01 maio 2023.

BONGHEZ, Simon. ***Internet & Web Development.*** 27 de abril de 2022. Disponível em: https://www.projectcubicle.com/internet-of-things-applications-in-industry/ Acesso em: 01 maio 2023.

CLEISON, Carlos. **Os Desafios da (*IoT*) Internet das Coisas no Brasil.** 26 jun 2017.Disponível em: https://medium.com/trainingcenter/os-desafios-da-*IoT*-internet-das-coisas-no-brasil-1052eb7155fb Acesso em: 11 maio 2023.

CLOUDFLARE. **O que é segurança da *IoT*? | Segurança dos dispositivos de *IoT*.** Disponível em: https://www.cloudflare.com/pt-br/learning/security/glossary/*IoT*-security/ Acesso em: 01 maio 2023.

CLOUD SECURITY ALLIANCE (CSA, 2016). ***Future-Proofing the Connected World: 13***
Steps to Developing Secure IoT Products, 2016. Disponível em: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/futureproofing-the-connected-world.pdf Acesso em: 10 maio 2023.

COMPUTERWORLD UK. **Especial *IoT*: 28 empresas com importantes avanços em internet das coisas.** 2019. Disponível em: https://itforum.com.br/noticias/especial-*IoT*-28-empresas-com-importantes-avancos-em-internet-das-coisas/ Acesso em: 22 nov. 2022.

FENG, X.; LAURENCE, T. Y.; LIZHE, W**.** ***Internet of Things. International Journal of Communication Systems***, v. 25, n. 9, p. 1101–1102, 2012.

FIGUEIRA, Vitor Pinheiro. **"Internet das Coisas": Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura.** 2016. 66 f. - Curso de Curso de Tecnologia em Sistemas de Computação, Universidade Federal Fluminense, Niterói, 2016. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/5150/TCC_VITOR_PINHEIRO_FIGUEIRA_FINA?sequence=1 Acesso em: 13 maio 2023.

FONTES, Edison; Cism; Cisa. **Segurança da Informação - O usuário faz a diferença**. São Paulo: Saraiva, 2006.

GOODIN, Dan. ***BrickerBot, the permanent denial-of-service botnet, is back with a vengeance.*** Ars Technica. 2017. Disponível em: https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/ Acesso em: 10 maio 2023.

IN CLUB. **9 Bons exemplos de como a Internet das Coisas (*IoT*) avança na Saúde – In Club.** 14 de julho de 2021. Disponível em: http://www.inclublicita.com.br/9-bons-exemplos-de-como-a-internet-das-coisas-*IoT*-avanca-na-saude/ Acesso em: 01 maio 2023.

KREBS, Brian. **DDoS on Dyn Impacts Twitter, Spotify, Reddit.** Krebs on Security. 2016. Disponível em: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/ Acesso em: 10 maio 2023.

LEITE, Leandro Rogério Corrêa. **Internet das Coisas (*IoT*): vulnerabilidades de segurança e desafios,** 2019. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana, Americana, 2019. Disponível em:

http://ric.cps.sp.gov.br/bitstream/123456789/3978/1/20192S_LEITELeandroRog%c3%a9rioCorr%c3%aaa_OD0763.pdf Acesso em: 10 maio 2023.

LIMA, Edilson. **“Internet das Coisas (*IoT*): Conheça 5 aplicações no cotidiano - LABORO**”. Faculdade Laboro, 17 de março de 2021. Disponível em: https://laboro.edu.br/blog/internet-das-coisas/ Acesso em: 01 maio 2023.

LIU, Yi; WANG, He; WANG, Junyu; QIAN, Kan; KONG, Ning; WANG, Kaijiang; ZHENG, Lirong; SHI, Yiwei; ENGELS, Daniel. ***Enterprise-Oriented IoT Name Service for Agricultural Product Supply Chain Management. International Journal of Distributed Sensor Networks.*** Volume 2015, Article ID 308165, 12 páginas.

MACHADO MEYER SENDACZ OPICE ADVOGADOS. **Lei 13.709/18: Lei de Proteção de Dados Pessoais**. São Paulo: Machado, Meyer, Sendacz e Opice Advogados, 2018.

MAGRINI, Eduardo. **A Internet das Coisas.** Rio de Janeiro. FGV Editora, 2018. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf Acesso em 22 nov. 2022.

MENEZES, Wander. **Rede Mirai: Ataques virtuais a dispositivos de *IoT* se tornam mais comuns**. 2017. Disponível em: https://itforum.com.br/noticias/rede-mirai-ataques-virtuais-dispositivos-de-*IoT*-se-tornam-mais-comuns/ Acesso em: 22 nov. 2022.

MASCARENHAS, P.; ARAÚJO, W. **Segurança da Informação: Uma visão sistêmica para implantação nas organizações.** João Pessoa: UFPB, 2009. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1 Acesso em: 22 nov. 2022.

RAZA, M. et al. ***A survey of password attacks and comparative analysis on methods for secure authentication.*** *World Applied Sciences Journal*, v. 19, p. 439–444, 01 2012.

SANNAPUREDDY, B. R. ***Pros & Cons of Internet Of Things* (*IOT*).** Disponível em: https://www.linkedin.com/pulse/pros-cons-internet-things-*IoT*-bhaskara-reddy-sannapureddy Acesso em: 02 maio 2023.

Segurança, Privacidade e Infraestrutura. 2016. 66 f. - Curso de Tecnologia em Sistemas de Computação, Universidade Federal Fluminense, Niterói, 2016.

SONNEMAKER, Tyler. ***Hackers breached security company Verkada and accessed 150,000 cameras inside Tesla, hospitals, and jails.*** Business Insider. Disponível em: https://www.businessinsider.com/verkada-hackers-breached-security-cameras-at-tesla-in-hospitals-jails-report-2021-3 Acesso em: 10 maio 2023.

RODRIGUES DE SOUSA, Daniel. ***IoT* com Arduino.** Slide Share, 2018. Disponível em: https://www.slideshare.net/danielrodriguesdesousa90/*IoT*-arduino Acesso em: 27 maio 2023.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação.** 4. ed. Brasília. 2012.

ZANI, Bruno. **As vulnerabilidades e necessidades de segurança em *IoT*.** 29/09/2016. Disponível em: http://www.securityreport.com.br/overview/mercado/vulnerabilidadesnecessidades-seguranca-*IoT*/#.XOSDjMhKjIU Acesso em: 10 maio 2023.

ZETTER, Kim. ***Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid***. Wired. Disponível em: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ Acesso em: 10 maio 2023.