Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Sistemas de Informação

Zero Trust Como Ferramenta de Segurança para Ambientes *E-Health*

Lucas Lino do Carmo Freitas

JUIZ DE FORA
JULHO, 2023

Zero Trust Como Ferramenta de Segurança para Ambientes *E-Health*

Lucas Lino do Carmo Freitas

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Sistemas de Informação

Orientador: Edelberto Franco Silva

JUIZ DE FORA

JULHO, 2023

Zero Trust Como Ferramenta de Segurança para Ambientes *E-Health*

Lucas Lino do Carmo Freitas

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutor em Ciência da Computação

Alex Borges Vieira
Doutor em Ciência da Computação

Luciano Jerez Chaves
Doutor em Ciência da Computação

JUIZ DE FORA
11 DE JULHO, 2023

Resumo

Em um mundo cada vez mais conectado, garantir a segurança em sistemas de saúde pode ser um grande desafio. Infraestruturas tradicionais baseadas na confiança em perímetro, acabam se mostrando insuficientes para garantir a segurança nesse ambiente. Uma vez que esse modelo funciona com a atribuição direta de confiança ao usuário, caso sejam comprometidas as credenciais ou o dispositivo do usuário, toda a rede se torna vulnerável. Assim, este trabalho propõe e avalia uma arquitetura *Zero Trust* para o aumento considerável de segurança em ambientes *e-health*. O modelo proposto é baseado na redução de privilégios e na análise de confiança do usuário para realizar o controle de acesso. Resultados obtidos através da avaliação em cenários distintos, comprovam a eficácia da proposta para o controle de acesso, ao proteger principalmente os recursos mais sensíveis.

Palavras-chave: Zero Trust, saúde, controle de acesso.

Abstract

In an increasingly connected world, ensuring security in e-health can be a significant challenge. Traditional perimeter-based infrastructures are not sufficient to guarantee security in this environment. Since this model works with direct attribution of trust to the user, the entire network becomes vulnerable if the user's credentials or device are compromised. Thus, this work proposes and evaluates a *Zero Trust* architecture for a considerable increase in security in *e-health* environments. The proposed model is based on privilege reduction and user confidence analysis to perform access control. Results obtained through the evaluation in different scenarios prove the proposal's effectiveness for access control, mainly protecting the most sensitive resources.

Keywords: Zero Trust, health, access control.

Agradecimentos

Primeiramente a Deus, pela minha vida e por me dar a inteligência para cursar o ensino superior.

Aos meus pais, que sempre foram minha base e meu apoio em todas as minhas conquistas.

Ao meu irmão, Rogério, que continuamente me incentivou a encarar meus desafios e me amparou nos momentos de desânimo.

Aos meus amigos, que trilharam essa jornada junto a mim, sempre me apoiando e encorajando.

Ao meu orientador, Edelberto Franco Silva, pela orientação, paciência e ensinamentos, o qual tornou possível o desenvolvimento deste trabalho.

Por fim, agradeço a todos os docentes da UFJF, que ao longo desses anos contribuíram para minha formação pessoal e profissional.

"Nossa maior fraqueza é a desistência. O caminho mais certeiro para o sucesso é sempre tentar apenas uma vez mais."

Thomas Edison

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

AAA	*Authentication, Authorization, and Accounting*
ABAC	*Attribute-Based Access Control*
CML	*Cisco Modeling Labs*
DDS	*Data Distribution Service*
IAM	*Identity and Access Management*
IDS	*Intrusion Detection System*
IA	Inteligência Artificial
IPS	*Intrusion Prevention System*
MEC	*Multi-access Edge Computing*
NIST	*National Institute of Standards and Technology*
PA	*Policy Administrator*
PDP	*Policy Decision Point*
PE	*Policy Engine*
PEP	*Policy Enforcement Point*
PoC	*Proof of Concept*
RbAC	*Risk-Based Access Control*
RBAC	*Role-Based Access Control*
TI	Tecnologia da Informação
ZT	*Zero Trust*
ZTA	*Zero Trust Architecture*

1 Introdução

1.1 Apresentação do Tema

Ao longo dos anos, a medicina vem sendo aprimorada e cada vez mais vem sendo empregado o uso de tecnologias, que auxiliam na luta contra diversos tipos de doenças e proporcionam melhores condições de vida e saúde para os pacientes (BARRA et al., 2006). Além disso, o uso da tecnologia revolucionaram os métodos e procedimentos tradicionais, possibilitando que consultas e procedimentos possam ser realizados de forma remota, e sistemas de Tecnologia da Informação e Comunicação (TIC) possibilitam que prontuários e todos os tipos de dados possam ser armazenados e gerenciados de forma muito mais fácil e ágil.

No entanto, a implementação de novos recursos tecnológicos, tem tornado os sistemas *e-health* alvos de invasores que buscam ter acesso a recursos e dados valiosos. Segundo Luh e Yen (2020), a área da saúde enfrenta uma "tempestade cibernética perfeita", onde cada vez mais são produzidos dados médicos, porém o investimento na segurança dos sistemas ainda se mantém insuficiente. Com isso, estima-se que pelo menos 90% das organizações do setor da saúde já sofreram algum tipo de violação de cibersegurança (DIAS et al., 2021).

De maneira geral, a infraestrutura comumente utilizada é baseada em perímetro, onde sua rede pode ser dividida em basicamente duas grandes áreas, a rede interna e a rede externa. Este modelo faz uso de confiança implícita, visto que quando o usuário passa pelo processo de autenticação e autorização, passa a ter acesso aos recursos da rede interna e ser considerado confiável. Esse modelo traz uma série de problemas, visto que, caso um invasor consiga se autenticar (utilizando-se de técnicas de phishing para obter credenciais de acesso, por exemplo), ele passa a ser considerado confiável e ter acesso a todos os recursos (TEERAKANOK; UEHARA; INOMATA, 2021).

Nesse sentido, a arquitetura *Zero Trust* (ZTA) surge como uma alternativa ao modelo legado para garantir mais segurança à infraestrutura. O modelo *Zero Trust* assume

que ninguém na rede é considerado totalmente confiável e que a autorização de acesso aos recursos deve ser revista a todo instante. Através da análise contínua do usuário, avaliando principalmente seu comportamento, o sistema atribui a ele um determinado nível de confiança, que deve ser atendido para que o acesso seja permitido. Isto torna o controle de acesso mais dinâmico e capaz de se adequar a diferentes cenários. com isso, este trabalho tem por finalidade fazer um estudo e simular a implementação da arquitetura *Zero Trust* em um ambiente *e-health*.

1.2 Contextualização

A tecnologia tem tido cada vez mais importância na área da saúde, e a partir dela uma riqueza de oportunidades inovadoras estão surgindo para agilizar os processos e suprir suas necessidades. Nos dias atuais é muito difícil imaginar a área da saúde sem o uso de inúmeros fatores tecnológicos. Nesta percepção, garantir sua segurança é de vital importância, visto que em nenhuma circunstância seus sistemas podem ser interrompidos ou terem seus dados roubados/alterados/sequestrados (COVENTRY; BRANLEY, 2018).

Em 2021, o setor da saúde foi um dos mais afetados por tentativas de invasões. De instituições públicas e privadas, foram mais de 39 mil tentativas de ciberataques, podendo representar perdas de dados ou não. O número chama muito a atenção pois fica a frente de outros setores com informações que também são consideradas valiosas, como indústrias de produção (36 mil) e instituições financeiras (25 mil), o que demonstra que a área da saúde está em foco quando falamos em ciberataques (MAIA, 2021).

Um exemplo que de impacto negativo dos ataques que pode ser observados no Brasil, é o ataque ao sistema do Conecte SUS que deixou a ferramenta indisponível por 13 dias, gerando prejuízos aos usuários e ao próprio governo, uma vez que não era possível realizar qualquer consulta ou cadastrar vacinas e qualquer outra informação no aplicativo (TORTELLA, 2021).

1.3 Descrição do Problema

O principal problema quando falamos em sistemas de gerenciamento de acesso tradicionais é que uma vez autenticado, o usuário adquire automaticamente uma confiança total no sistema, sendo atribuído à ele o acesso, conforme definidos nas diretrizes.

A grande questão ligada aos modelos tradicionais é que ela é baseado em um perímetro físico/lógico, ou seja, normalmente é estabelecido uma divisão entre rede interna (considerada como uma área confiável) e uma rede externa (considerada como uma área não confiável), e entre elas uma série de conjunto de defesa (e.g., *firewall*, *proxy*, IDS, IPS) é estabelecido para garantir a segurança entre as duas grandes áreas (SOUZA, 2013).

O principal problema dessa metodologia é que basta que um invasor consiga se autenticar como um usuário ou através do controle de um dispositivo da empresa, para adquirir também total confiança do sistema. Por mais que as empresas invistam em políticas de segurança e treinamentos, confiar ao usuário uma boa gestão dos recursos nem sempre garante a segurança, uma vez que ele pode ser facilmente ludibriado por arquivos maliciosos disfarçados de conteúdos reais e com apenas um clique, pode comprometer toda a segurança de uma instituição. Ataques desse tipo representam uma ameaça a todas as organizações e medidas de segurança precisam ser tomadas para assegurar a integridade do sistema.

1.4 Justificativa/Motivação

Devido à grande relevância dos sistemas *e-health* e os problemas neles enfrentados, em especial ao modelo de perímetro, a justificativa deste trabalho se baseia na importância de se garantir a segurança nos sistemas da área da saúde. Em consequência da falta de investimentos e inúmeras vulnerabilidades presentes nestes sistemas, tem se atraído cada vez mais invasores que buscam explorá-los (ZEADALLY; ISAAC; BAIG, 2016).

Pelo fato de Sistemas *e-health* lidarem diretamente com a saúde das pessoas, torna essa necessidade de proteção contra acessos não autorizados ainda maior. A interferência direta de invasores podem causar impactos significativos sobre o tratamento de pacientes e por consequência, em suas vidas.

Neste sentido, com a implementação do *Zero Trust* uma série de benefícios são agregados à proteção dos recursos, dentre eles o maior ganho está relacionado ao aumento considerável na segurança da informação, pois a metodologia cerca um dos principais problemas ligados à segurança: a confiança estabelecida ao usuário.

1.5 Objetivos

1.5.1 Geral

Este trabalho tem como principal objetivo apresentar a metodologia *Zero Trust*, sob seus aspectos teóricos e práticos, assim como demonstrar os benefícios obtidos através de sua implementação em um ambiente simulado e padronizado com definições ligadas à saúde.

Após um levantamento sobre princípios, pilares e metodologia de implementação, será desenvolvido um ambiente virtual similar a um ambiente real sobre os aspectos do *e-health*. Nesse ambiente será implementado um algoritmo de *Zero Trust* e através do estabelecimento de políticas de segurança, o sistema será submetido a testes.

1.5.2 Específicos

Os objetivos específicos para desenvolvimento deste trabalho são:

- pesquisar e estudar toda fundamentação teórica para embasamento deste trabalho;
- pesquisar as necessidades específicas de segurança na área da saúde;
- implementar uma arquitetura *Zero Trust* em um ambiente simulado, que atenda aos níveis de segurança para proteção de acesso aos recursos e dados;
- elaborar e executar testes no ambiente implementado.

1.6 Organização

Esta monografia está organizada em seis capítulos, além desta introdução. O Capítulo 2 apresenta a fundamentação teórica de conceitos importantes, como: *Device Fingerprint*,

gestão de identidade e acesso, métodos de autenticação, métodos de autorização e *Zero Trust*. O Capítulo 3 apresenta os trabalhos relacionados à implementação da arquitetura ZT e modelos de controle de acesso. O Capítulo 4 detalha o processo de desenvolvimento. No Capítulo 5 são apresentados os testes e resultados obtidos. Por último, o Capítulo 6 apresenta as conclusões.

2 Fundamentação Teórica

Neste capítulo são abordados conceitos importantes para a compreensão do trabalho desenvolvido neste artigo. A Seção 2.1 apresenta o *Device Fingerprint* e como é utilizado para incremento da segurança. Na Seção 2.2 é descrita a gestão de identidade e acesso, juntamente com os processos de autenticação (Seção 2.3) e autorização (Seção 2.4). Por fim, na Seção 2.5 é apresentada a conceitualização sobre os princípios do *Zero Trust*.

2.1 Device Fingerprint

Device Fingerprint (DFP) é uma técnica utilizada para identificar dispositivos eletrônicos, através de análises com base nas características dos dispositivos utilizados (XU et al., 2015). Assim como cada pessoa possui impressões digitais únicas, os dispositivos também possuem uma combinação única de atributos que podem ser usados para identificá-los.

Essa tecnologia é baseada na coleta de informações sobre o dispositivo, como o sistema operacional, o fuso horário, a resolução da tela, os plugins instalados e outros detalhes técnicos (ALACA; OORSCHOT, 2016). Essas informações são combinadas para criar uma "impressão" exclusiva, que pode ser usada para distinguir um dispositivo de outros.

O Device Fingerprint é usado principalmente para aumentar a segurança contra falsificações de dispositivos, visto que é extremamente difícil de se falsificar todas as características necessárias (XU et al., 2015). Desta forma, simplesmente clonar o MAC de um dispositivo não será o suficiente para se passar por ele. Ao analisar os atributos do dispositivo durante um acesso a um recurso, por exemplo, é possível identificar um dispositivo legítimo através da análise dos acessos anteriores.

2.2 Gestão de Identidade e Acesso - IAM

A Gestão de Identidade e Acesso (IAM) pode ser definido como um conjunto de processos e métodos cujo objetivo é fornecer segurança adequada para a identidade, dados e recursos da organização, por meio de políticas e procedimentos empregados (SHARMA; SHARMA; DAVE, 2015).

A identidade no mundo digital representa uma série de informações do usuário e essas informações podem ser usadas para diversos fins. O gerenciamento de identidade é uma metodologia de representação e reconhecimento de identidades no mundo digital, garantindo a integridade das informações (LEANDRO et al., 2012).

No processo de gerenciamento de identidade, se faz muito presente os processos de autenticação, autorização e auditoria (AAA). Começando pelo processo de autenticação, ele é responsável por assegurar que determinado usuário ou dispositivo é quem realmente afirma ser. Já o processo de autorização garante que, uma vez autenticado, o usuário ou dispositivo só tenha à sua disposição os recursos ao qual está permitido a usar. Por fim, a auditoria é o processo de análise das operações, onde através da coleta dos dados relacionados ao uso dos recursos pelos usuários, como quem acessou, quando acesso, o que acessou, entre outros, se possa aferir sua qualidade. Alguns métodos de autenticação e autorização serão descritos nas Seções 2.3 e 2.4 respectivamente.

2.3 Métodos de Autenticação

O processo de autenticação consiste em mecanismos que garantem a autenticidade dos usuários finais que estão presentes em determinados contextos, ou seja, garante que o usuário é quem ele diz ser. Para isso, uma série de métodos de avaliação podem ser aplicados nesse processo de validação, sendo cada um mais ou menos recomendado de acordo com o contexto organizacional para sua aplicação.

2.3.1 Autenticação por Senha

A autenticação em senha é o meio de identificação baseado no conhecimento, onde normalmente o usuário precisa informar uma combinação de um identificador (e. g., nome,

e-mail, cpf, matrícula) e uma palavra chave, que serão validados por um servidor, permitindo ou não, o seu acesso (LIAO; LEE; HWANG, 2006).

Este método se tornou um dos mais utilizados pela sua facilidade de implementação, porém a autenticação por senha trouxe uma série de problemas de segurança, onde a principal falha se encontra no fator humano (LAL; PRASAD; FARIK, 2016). Podemos citar como principais falhas humanas: o esquecimento, reutilização de senha em vários sistemas, senhas facilmente adivinhadas, compartilhamento de senha com outras pessoas, anotações das senhas, dentre outros.

2.3.2 Autenticação por *Token*

A autenticação por *token* é um método de autenticação baseada em "o que o usuário possui", onde o usuário utiliza um código único de acesso para realizar o processo de identificação. A autenticação por *token* pode ser realizada com *token* baseado em *hardware* ou *software* (MIZRACHI, 2021).

A autenticação de *token* baseado em *hardware* é feita com o uso de dispositivos físicos que permitem o reconhecimento do usuário. Normalmente este tipo de autenticação é utilizado para aumento de segurança em autenticação multifator.

Já a autenticação de *token* baseada em *software* ocorre primeiramente com a autenticação feita por outros meios (comumente utilizado a autenticação por senha), onde o sistema gera um código assinado e único e o repassa ao usuário. Em posse deste código, para suas próximas autenticações, precisará apenas utilizar o *token* para realizar sua identificação. Esses *token* normalmente possuem um prazo de validade que determina o tempo em que poderá ser utilizado e caso o *token* ultrapasse o prazo, será necessário realizar todo o processo novamente.

2.3.3 Autenticação Biométrica

A autenticação biométrica é um método que se caracteriza pela identificação com base em características físicas e/ou comportamentais do usuário. Podemos citar como características físicas o reconhecimento facial, impressão digital, reconhecimento da íris, dentre outros, e para as características comportamentais podemos citar a assinatura, modo de

digitação, entonação da voz, etc (BHATTACHARYYA et al., 2009). O uso de múltiplas tipos de autenticação biométrica podem ser combinados para aumentar a confiabilidade da identificação.

Para se escolher uma característica para autenticação, os seguintes fatores devem ser levados em consideração (DHARAVATH; TALUKDAR; LASKAR, 2013):

- universalidade: todos os usuários que utilizarão o sistema devem possuir o traço biométrico;
- permanência: a característica biométrica não deve ser facilmente alterada/modificada ao longo do tempo;
- mensurabilidade: a coleta e o processamento dos traços biométricos deve ocorrer de maneira rápida e fácil, permitindo análise e comparações posteriores;
- singularidade: a característica biométrica deve ser única e permitir distinguir facilmente uma pessoa da outra;
- aceitabilidade: por se tratar de uma característica particular, a coleta do traço deve ser aceitável pelo grupo de usuários;
- confiabilidade: o traço biométrico não deve ser possível mascará-lo, a fim de que uma pessoa se passe por outra;
- evasão: a característica biométrica não deve ser reproduzível por outros meios.

Quando um usuário precisa se autenticar, ele fornece uma "amostra biométrica" ao sistema, que à processará e gerará um modelo que será comparado com o armazenado no sistema (DHARAVATH; TALUKDAR; LASKAR, 2013).

O modelo de autenticação biométrica tem se apresentado como uma forma mais confiável e eficaz de verificação de identidade, uma vez que as características dos usuários são difíceis de se fraudar ou copiar (JAIN; NANDAKUMAR, 2012). Outra vantagem do modelo de autenticação biométrica é que, por se tratar de uma característica única do usuário, os problemas clássicos de esquecimento e roubo de identificadores não são aplicáveis (DHARAVATH; TALUKDAR; LASKAR, 2013).

2.4 Métodos de Autorização

Os modelos de autorização por sua vez são indispensáveis quando falamos de gestão de acessos. Uma vez combinado com modelos de autenticação, os mecanismos de autenticação garantem que os usuários ou dispositivos já com suas identidades verificadas e atestadas, estão autorizados a acessar determinados recursos. Estando liberados, os mecanismos de autorização se certificam de que o usuário ou dispositivo tenha acesso aos recursos que lhes são correspondentes, de forma ágil e sem interrupções.

2.4.1 Controle de Acesso Baseado em Papéis - RBAC

O Controle de Acessos Baseados em Papéis (RBAC) não é uma novidade propriamente. Criado na década de 70, o modelo consiste na atribuição de acessos aos usuários com base nos papéis que ele possui, ou seja, para cada atribuição (cargo, função, atividade e afins) o sistema de controle fará determinada liberação do acesso ao usuário. Esse modelo propicia uma facilidade maior na definição de políticas de acesso, assim como permite a fácil migração entre papéis, se adaptando a novos cenários como promoções, implementação de novos sistemas e afins (OBELHEIRO; FRAGA; WESTPHALL, 2001).

Conforme demonstrado na Figura 2.1, temos duas correlações principais, denominadas de UP (entre usuários e papéis) e PA (entre papéis e autorizações). Na correlação UP, temos um relacionamento onde um usuário pode possuir vários papéis atribuídos a ele e por outro lado temos um papel que também pode ser atribuído a diversos usuários. Já na correlação PA temos uma relação onde os papéis são atribuídos a determinadas autorizações. Desta forma, quando um usuário inicia uma seção, através dos papéis atribuídos a ele, é possível determinar suas autorizações e por consequência, estabelecer quais recursos ele pode ter acesso (GUERRA; PAIVA; FERNANDES, 2004).

O processo de gerenciamento baseado em papel se apresenta como muito mais flexível a outros métodos uma vez que a atribuição não é feita diretamente ao usuário e sim a um determinado papel. Havendo a necessidade de acrescentar, remover ou modificar as atribuições do usuário (ou seja, ele adquire ou perde responsabilidade sobre algum processo), basta conceder/revogar sua atribuição ao papel. Outro ponto de flexibilidade é que qualquer alteração no papel será refletida automaticamente a todos os usuários que

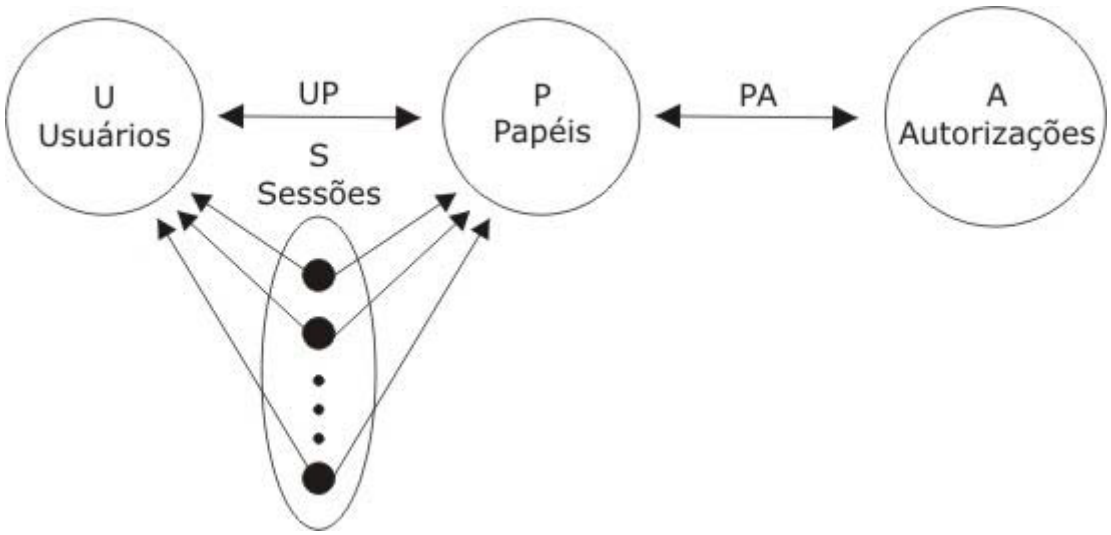


Figura 2.1: Estrutura Esquemática do Modelo RBAC (GUERRA; PAIVA; FERNANDES, 2004)

o contenham (UEDA, 2012).

2.4.2 Controle de Acesso Baseado em Atributos - ABAC

No modelo de Controle de Acessos Baseado em Atributos (ABAC) o sistema utiliza de atributos em torno da operação para determinar a validade de determinada solicitação de acesso, usando esses atributos como base para a liberação ou não do acesso ao recurso. Os atributos considerados podem ser os mais diversos, mas comumente se trabalha com os três principais, que são: atributos de sujeito, objeto e ambiente (HU et al., 2015).

Atributos de sujeito são atributos relacionados aos componentes que podem diretamente atuar sobre objetos, como usuários, dispositivos e sistemas, sendo avaliado os atributos associados a esses componentes como cargo, nome e afins. O atributo de objeto por sua vez, considera os componentes que sofrem diretamente ações do sujeito, podendo ter como atributos seu título, autor e outras informações que podem ser associadas diretamente ao objeto. Por fim, os atributos de ambiente consideram informações ao sistemas, como hora atual, dia da semana e afins (SHEN; HONG, 2006).

Para a liberação nesse modelo, o usuário faz uma requisição de acessos a determinado recurso e para que sua solicitação seja aprovada, os atributos correspondentes ao recurso devem ser atendidos pelos atributos do usuário. Após um conjunto de decisões baseadas nos atributos especificados, o usuário terá seu acesso permitido caso satisfaça a

todas as condições (CREMONEZI et al., 2021).

Este modelo de controle de acesso se torna muito interessante pois torna a administração das regras de acesso mais dinâmica, visto que para ajustar as permissões, basta alterar os valores dos atributos desejados (HU et al., 2015).

2.4.3 Controle de Acesso Baseado em Risco - RbAC

A análise de riscos é algo que está presente em toda a organização. Avaliar os riscos de uma determinada ação (seja no presente ou no futuro) é indispensável quando falamos sobre gestão de acessos. Por isso, o modelo de Controle de Acessos Baseado em Riscos (RbAC) considera todas as variáveis envolvidas para promover uma análise e estudo dos riscos, e com base nas probabilidades e potenciais danos de uma ocorrência, determina-se a validação ou não da liberação de determinado acesso (ATLAM et al., 2017).

Geralmente o fator risco é considerado como algo estático no processo, mas a metodologia de gerenciamento de acessos com base em risco busca trazer uma abordagem mais dinâmica, trazendo decisões como no mundo real (SANTOS; WESTPHALL; WESTPHALL, 2014).

O processo de análise de risco para o controle de acessos pode se dar de duas formas, a qualitativa ou quantitativa. No modelo qualitativo, há a necessidade da interferência de um especialista para que valorize os riscos e a partir dessa valorização, seja possível aplicar diferentes escalas de graduação. Enquanto no método quantitativo, procura-se atribuir números que representam o risco envolvido. O cálculo geralmente utilizado em métodos quantitativos para se definir o risco é dado pela fórmula $R = P \cdot I$, sendo R o risco, P a probabilidade da sua ocorrência e o I o impacto deste risco (SANTOS et al., 2013).

Para a análise de risco, pode-se utilizar uma base histórica de eventos e a partir dela, definir com maior facilidade o impacto no processo (SANTOS; WESTPHALL; WESTPHALL, 2014).

2.5 *Zero Trust*

Focada na proteção dos recursos, o *Zero Trust* (ZT) trabalha com a ideia de que a confiança no usuário não deve ser estabelecida de forma fixa ou determinada de acordo com sua localização no perímetro, mas analisada e atribuída continuamente. O ZT não é um produto em si, mas um conjunto princípios que buscam trazer uma maior segurança aos recursos da organização, onde promove a proteção na transação de informações, a integralidade dos dados e a certificação/autorização dos usuários ou dispositivos que acessam os recursos (ROSE et al., 2020).

A metodologia se baseia em oferecer apenas o mínimo de privilégios possíveis para realizar sua tarefa, ao contrário dos modelos baseados em perímetro, onde o usuário recebe privilégios ao máximo, muito além do necessário para a sua atividade na maioria dos casos. Se nos modelos tradicionais a filosofia era "confiar porém verificar", no ZT a idéia é "nunca confiar e sempre verificar", de modo a assumir que um invasor está sempre presente na rede (AWAN et al., 2023; ROSE et al., 2020).

Para mitigar os efeitos da incerteza de um usuário com "plenos poderes", o *Zero Trust* busca autenticar o usuário e conceder privilégios gradativamente de acordo com seu uso, mantendo a disponibilidade dos recursos e não gerando qualquer empecilho ao usuário ou a organização (ROSE et al., 2020).

2.5.1 Princípios do *Zero Trust*

Para Rose et al. (2020), ao se considerar adotar a metodologia de *Zero Trust* para qualquer organização, é importante que se conheça e respeite os princípios abaixo durante o processo de implementação:

- se tratando de redes corporativas, todos os dispositivos que a compõem devem ser considerados, sendo todas as fontes de dados vistas como recursos, sejam corporativos ou pessoais;
- todo dispositivo que transmita na rede, independente da sua localização, deve atender aos mesmos requisitos que se aplicam a todos os dispositivos;

- os acessos a recursos na rede devem ser analisados individualmente por sessão para a liberação de acessos, mantendo o mínimo de privilégios possíveis;

- a autorização de acessos a recursos corporativos não pode ser estática, esse processo deve considerar uma série de atributos no ato da validação. A verificação deve seguir os padrões estabelecidos na política de segurança, desde a identificação do usuário à características como sistema operacional e horários;

- integridade e segurança da rede são pontos indispensáveis e por isso precisam ser monitorados e acompanhados de perto pelas organizações. A metodologia *Zero Trust* deve estabelecer condições para que o acompanhamento e mitigação de riscos ocorra;

- no processo de permissão de acessos, é indispensável que se aplique métodos rigorosos para autenticação e autorização, antes que o acesso seja permitido. Sistemas de gerenciamento de identidades devem ser utilizados frequentemente para apoiar os sistemas de reautenticação e reautorização;

- as políticas de segurança precisam evoluir de acordo com as práticas dos usuários, por isso se faz muito importante a coleta constante de dados relacionados ao uso da rede e esses dados poderão ser aplicados diretamente para o aprimoramento da segurança.

2.5.2 Arquitetura *Zero Trust*

A arquitetura ideal para a implantação do *Zero Trust* pode variar seus componentes de acordo com as necessidades da organização. No entanto, o Instituto Nacional de Padrões e Tecnologia (NIST), do Departamento de Comércio dos Estados Unidos, definiu e apresentou os componentes lógicos básicos de uma arquitetura ideal para implantação ZTA (*Zero Trust Architecture*), bem como suas interações, que são compostas por: Ponto de aplicação de políticas (PEP) e Ponto de decisão da política (PDP), este último dividido em dois componentes, Mecanismo de política (PE), Administrador de política (PA), conforme Figura 2.2 (ROSE et al., 2020).

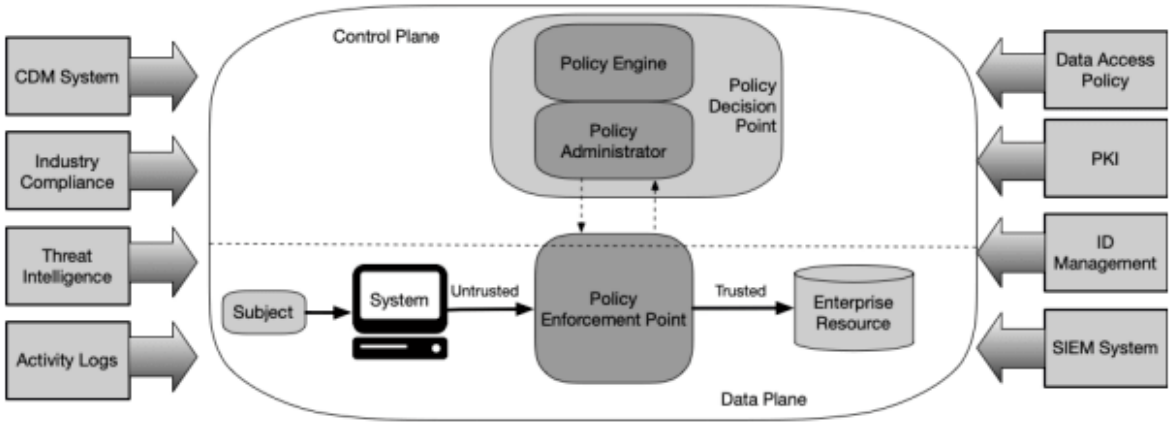


Figura 2.2: Componentes lógicos da Arquitetura *Zero Trust* (ROSE et al., 2020)

O PDP é responsável pela permissão ou negação de acesso aos recursos da organização. Divididos em dois componentes lógicos, o PE é responsável pela decisão final de conceder, negar ou revogar o acesso a um determinado recurso. Para isso, o PE utiliza da política de segurança da organização e fontes externas, como entrada de dados para orientar a tomada de decisão. O PA por sua vez, é responsável pelo gerenciamento da comunicação, autenticação, e transmitir ao PEP as decisões de acesso tomadas pelo PE (ROSE et al., 2020).

Por fim, PEP é o componente que promove a comunicação entre o usuário e os recursos, bem como monitorar e encerrar a conexão. Ao receber uma solicitação, o PEP se comunica e encaminha a requisição para o PA, e após sua decisão, habilita ou encerra a comunicação entre usuário e recurso. Em outras palavras, o PEP atua como uma porta de controle de acesso (TEERAKANOK; UEHARA; INOMATA, 2021).

3 Trabalhos Relacionados

Neste capítulo é apresentado alguns trabalhos relacionados que buscaram, de alguma forma, implementar e estabelecer métodos para autorização de acesso à recursos. Para os ambientes de saúde, muito já se foi discutido sobre a importância de se garantir a segurança, privacidade e integridade de seus sistemas. A Seção 3.1 aborda os trabalhos que propuseram sistemas que implementam o *Zero Trust* como meio para gerir o controle de acesso em ambientes de saúde. A Seção 3.2 apresenta a implementação da ZTA em outro ambiente que, apesar de não tratar diretamente da área da saúde, serve também para demonstrar a importância e a proteção do modelo proposto. A Seção 3.3 discute sobre trabalhos que implementam algum método de controle de acesso, em especial o ABAC e RbAC.

3.1 Implementações da Arquitetura *Zero Trust* em Ambientes *E-Health*

No trabalho de Tyler e Viana (2021), os autores propuseram um sistema de segurança para ambientes de saúde baseado na arquitetura *Zero Trust* , através de simulação da rede pelo *Cisco Modeling Labs* (CML). A fim de se identificar qual seria a melhor estratégia baseada no modelo *Zero Trust*, foram criadas redes virtuais através do CML e, através dessa ferramenta foram criadas e testadas estruturas com micro segmentações e topologias de seguranças, associadas aos controles de acessos. Segundo os autores, após a criação das redes virtualizadas, foram enviados pacotes de dados entre diversos dispositivos a fim de se verificar e testar o nível de acessibilidade de cada dispositivo. Através desse teste foi avaliado principalmente quesitos ligados a segurança, onde se checou se cada dispositivo que compõe o teste, tinha apenas as permissões necessárias para acessar os recursos os quais foram previamente autorizados. Durante a realização dos testes era necessário que as interações em toda rede e todos os dispositivos que a compunham fossem analisados, para

isso foi utilizado o *Wireshark*[1] para essa função. Os testes em si foram iniciados a partir do disparo de pacotes tendo como origem os dispositivos médicos e toda a rede como destino, e para se garantir a conformidade do teste, foram extraídas amostras antes e depois da implementação do ZT. Após a realização dos testes propostos, os autores realizaram testes comparativos com as informações que foram coletadas a fim de determinar se houve ou não uma variação (diminuição ou aumento) na latência, após a implementação da metodologia na rede.

O trabalho de Ali, Gregory e Li (2021) aborda a Computação de Borda de Multi-acesso (MEC), onde através da coleta de informação é possível se tomar decisões de segurança com maior assertividade seguindo os princípios de *Zero Trust*. O trabalho proposto teve como base um sistema que se baseia em três camadas, sendo elas: equipamento de usuário, borda (responsável por rotinas de rede como proteção de *firewall*, conexão sem fio, terminação de rede, tradução de protocolos e afins) e nuvem (responsável por fornecer serviços, aplicações e armazenamento para dispositivos). Os testes ocorreram através de uma Prova de Conceito (PoC) partindo do princípio que a metodologia é válida e sua implementação possui um grande potencial de benefícios quando o *Zero Trust* é adotado. Com o resultado de todos os testes, a simulação foi avaliada quanto aos quesitos de taxa de sucesso, falha e o tempo necessário. Após a avaliação dos resultados obtidos, os autores apontaram que a metodologia se mostrou muito promissora. Começando pela taxa de sucessos no MEC com *Zero Trust* que foi de 80%, enquanto sem o ZT a taxa caiu para cerca de 54%. A taxa de erro por sua vez foi de 28% no MEC com *Zero Trust*, contra 54% sem o ZT. O MEC com *Zero Trust* também se destacou no quesito de tempo de autenticação, sendo 0,5ms mais rápido que o modelo sem o ZT, sendo segundo os autores, devido ao algoritmo leve para autenticação de tráfego legítimo e ilegítimo. Através da implementação de um modelo de *Zero Trust* com um algoritmo leve de autenticação, os autores mostraram que a metodologia se faz uma abordagem muito rica para o aumento da segurança dos dados, além da redução considerável nos riscos.

[1] https://www.wireshark.org/

3.2 Implementação da Arquitetura *Zero Trust* em Outro Ambiente

No trabalho de D'Silva e Ambawade (2021), os autores propuseram também a implementação da arquitetura *Zero Trust* em ambientes organizacionais, porém utilizado para acessos realizados via web. O modelo apresentado foi desenvolvido com *Kubernetes* e testado em um ambiente simulado, onde a arquitetura foi dividida em 5 blocos principais: cliente, servidor *proxy*, servidor AAA, aplicação e o controle de acesso. O cliente é quem realiza as requisições. O servidor *proxy* filtra essas requisições e as redireciona para o servidor AAA. O servidor AAA é responsável por realizar a autenticação e executar a permissão de acesso. O servidor de controle de acesso implementa uma combinação do modelo de controle de acesso baseado em função e atributos e é responsável por tomar a decisão final de autorização e repassá-la ao servidor AAA. Por fim, a aplicação é o recurso final ao qual o cliente deseja acessar. Para os testes, os autores apontam uma série de ataques (como infecção de dispositivos, invasão do perímetro, falsificação de identidade, inundação do tráfego, dentre outros), ao qual o modelo proposto deve apresentar uma resposta, porém a resolução desses testes não foram apresentados. Ainda sim, os autores concluíram como resultados que a ZTA se mostrou como uma opção robusta para aumentar a segurança cibernética.

3.3 Modelos de Controle de Acesso em Ambientes *E-Health*

O trabalho de Kim, Kim e Alaerjan (2021) propuseram um sistema para controle de acesso à registros médicos, fundado em Controle de Acesso Baseado em Atributos. Os autores apontam que um dos principais possíveis ganhos ao se utilizar o ABAC está na maior flexibilização das definições das políticas de acesso em um ambiente de saúde. No sistema mostrado foi utilizado um Sistema de Distribuição de Dados (DDS), um padrão utilizado para criptografia dos dados, registro de eventos, autenticação de identidade dos usuários e autorização de acessos, onde o ABAC seria empregado como suplemento de segurança.

Os autores definiram 4 entidades principais para o trabalho: participante (identificada por *token*), atributo, condições do ambiente e definição de regras utilizadas para tomada de decisão. Ainda foi definido também, uma árvore de decisão, que contém as políticas estabelecidas e um conjunto de regras. O sistema foi desenvolvido e testado em um ambiente simulado, onde os dispositivos já se encontram autenticados e sua comunicação só ocorre mediante permissão do ABAC. A avaliação do sistema feita pelos autores ocorreu em cima da verificação em relação a sua eficácia, escalabilidade e eficiência. Quanto à eficácia, os autores concluíram que o uso do ABAC reforçou com êxito o controle de acesso. Para a escalabilidade e eficiência, a avaliação foi feita em cima do tempo gasto na comunicação, variando o número de requisições de 150 à 1050 simultâneas, onde considerando o máximo testado, o tempo de comunicação foi de 40,6 milissegundos. Por fim, os autores concluíram que o ABAC atendeu as necessidades para aplicação em um ambiente de saúde, porém ressaltam ainda que o modelo centralizado apresentado pode sofrer com sobrecargas, e que mais estudos devem ser realizados para aumentar sua confiança.

Por meio da aplicação de lógica *fuzzy*, o trabalho de Li, Bai e Zaman (2013) propuseram um sistema para controle de acesso baseado em risco em ambientes *e-health* em nuvem. O modelo utiliza de lógica difusa para analisar as requisições e tomar decisões de acesso à informações médicas, ou seja, ela analisa o dano potencial para permitir ou não o acesso. Para realizar a análise, os autores utilizaram um conjunto de 3 entradas em cada requisição: nível de gravidade da ação (classificados como baixo, médio ou alto), sensibilidade dos dados requeridos (classificados como não sensível, sensível e altamente sensível) e um histórico de riso de acesso ao recurso pelo usuário. Após a análise dessas entradas, o sistema classifica o risco de acesso como insignificante, baixo, moderado, alto ou inaceitavelmente alto, com base nas regras *fuzzy* definidas. Ao final do trabalho, os autores realizaram testes com diferentes entradas e classificaram o modelo proposto como eficaz para a previsão do impacto e o gerenciamento de segurança.

3.4 Considerações Finais

Neste capítulo foram apresentados os principais trabalhos relacionados ao tema, dando uma abordagem tanto do ponto de vista teórico quanto do ponto de vista da sua imple-

mentação. Através da exposição destes trabalhos é possível se observar o quão importante se faz a implementação de métodos para garantir a segurança dos recursos, em especial aos ligados à área da saúde.

Através dos trabalhos relacionados é possível se ter uma ideia de que o ZT se apresenta como um potencial para ser superior às metodologias tradicionais (baseadas em perímetro), tanto nos quesitos de taxa de sucesso/erros, estabilidade e escalabilidade. Outro ponto que será altamente aplicável a este trabalho são os modelos de gestão de acessos baseados em riscos e atributos, que poderão ser implementados juntamente à ZT.

4 Desenvolvimento

Neste capítulo são apresentadas a metodologia e as etapas de desenvolvimento deste trabalho. Para isso, a Seção 4.1 apresenta uma visão geral da arquitetura, seus componentes, e o processo de tomada de decisão. A seção 4.2 apresenta os recursos administrados pelo ZT e uma análise de sensibilidade. Na seção 4.3 é descrito o processo para cálculo de confiança.

4.1 Visão Geral

O desenvolvimento deste trabalho tomou como base a definição da arquitetura base do *Zero Trust* definida em Rose et al. (2020). Todo processo consiste em um conjunto de usuários ou dispositivos que buscam acessar determinados recursos, e entre essas duas partes, o sistema ZT analisa as requisições, determina o nível de confiança do usuário e a sensibilidade do recurso para tomar sua decisão.

Para o desenvolvimento, a implementação foi dividida em três partes: cliente, recursos e sistema de controle de acesso. Cada uma destas partes foram desenvolvidas utilizando a linguagem de programação Python[2], uma linguagem que já é muito utilizada para análise de dados e desenvolvimento de backends.

Desta forma a idéia principal é que, para que um usuário possa acessar um determinado recurso, sua requisição obrigatoriamente deve passar pelo sistema de controle de acesso, que determinará, com base na análise de seu uso, um nível de confiança e por fim determinar se o usuário pode ou não ter acesso ao recurso requerido.

Conforme demonstrado na Seção 2.5.2 e na Figura 4.1, a arquitetura do *Zero Trust* proposto é composta por três módulos principais: PEP, PDP e PIP. O PEP é responsável por receber a requisição, fazer todo controle de seção, enviar o pedido ao PDP e aplicar a decisão tomada. O PDP é responsável por realizar o controle de acesso com base nas políticas definidas. E por fim, o PIP é responsável por reunir todas as

[2]⟨https://www.python.org/⟩

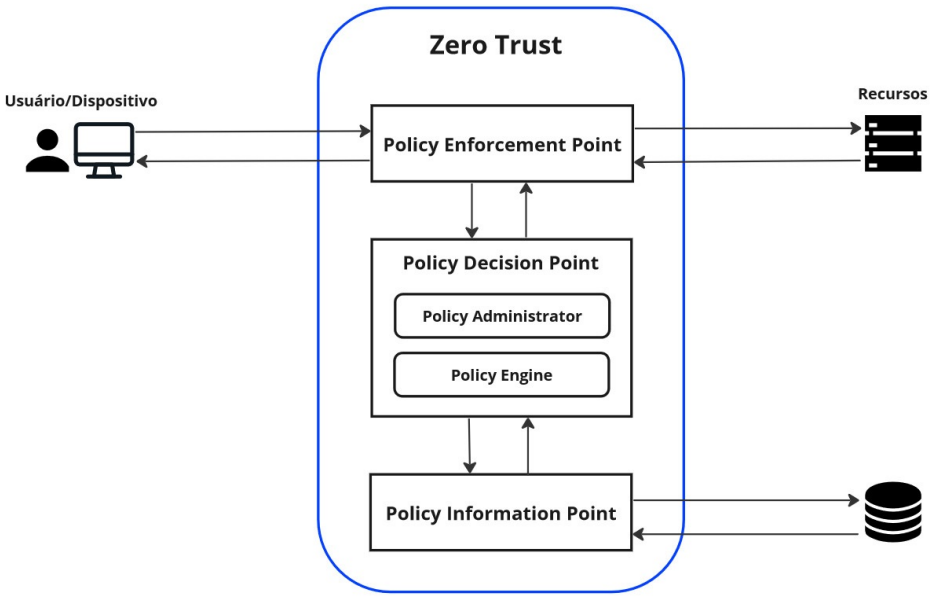


Figura 4.1: Arquitetura do *Zero Trust* (ROSE et al., 2020)

informações necessárias para que o PDP possa analisar o pedido. Ainda em conjunto com esta estrutura, foi utilizado um banco de dados para armazenamento das informações, detalhado na Seção 4.4.

Para simulação da rede, cada uma das partes (usuários, recursos e *Zero Trust*) foram executados como um "processo", onde a comunicação entre eles se deu através de sockets[3]. Este modelo foi escolhido visto que o objetivo é avaliar a assertividade na tomada da decisão, não levando em consideração métricas de rede.

O processo de autenticação foi feito a partir do fornecimento de um identificador e senha pelo usuário. Após validados, o sistema gera um *token* único com validade de 3 dias, que será utilizado para sua identificação nos demais acessos.

Para determinar o acesso aos recursos, o ZT proposto toma sua decisão através do cruzamento de duas informações, ambas em um intervalo de 0 a 100. Primeiramente é calculado a confiança do usuário, dispositivo e histórico e em seguida definido a sensibilidade quanto ao recurso desejado. O cálculo da confiança e a definição da sensibilidade é detalhado nas Seções 4.2 e 4.3 respectivamente. Com essas informações, o acesso pode ser permitido, negado, ou solicitado uma reautenticação, conforme ilustrado na Figura 4.2.

Desta maneira, analisando continuamente a confiança do usuário, os recursos mais

[3]Socket: Um endpoint composto por "IP:PORT" utilizado para identificar um processo específico.

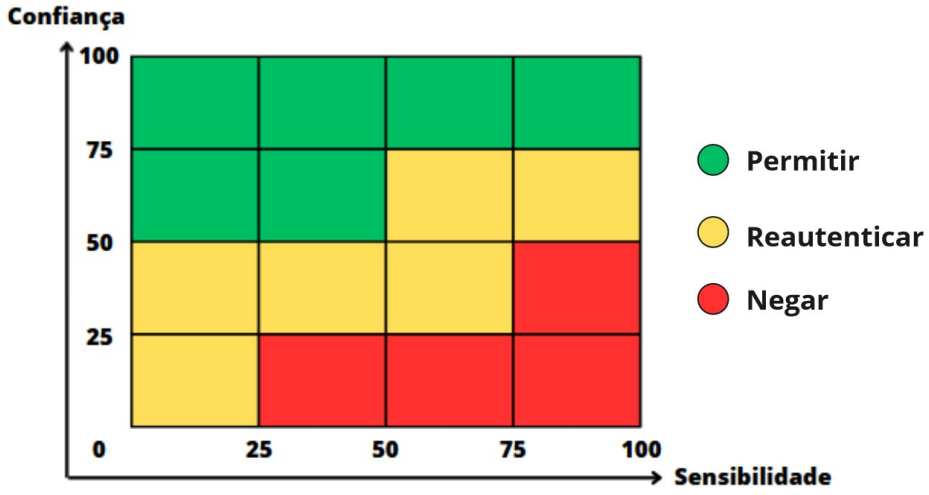


Figura 4.2: Permissões atraves da Confiança X Sensibilidade

sensíveis só estarão disponíveis a usuários com a confiança mais elevada, e os recursos menos sensíveis poderão ser acessados por usuário com confiança menores. Portanto, neste modelo o maior desafio é determinar, em tempo de execução, a confiança do usuário e detectar possíveis anormalidades. O código fonte desenvolvido neste trabalho está disponível publicamente no GitHub[4].

4.2 Recursos e Sensibilidade

Com o objetivo de explorar os ambientes e-health e aproximar-se de um ambiente real, 5 recursos principais, comumente utilizados na área da saúde, foram escolhidos para compor os recursos disponíveis. Eles não serão propriamente desenvolvidos, mas serão utilizados pelo ZT para o controle de acesso. Segue a lista de recursos escolhidos, com uma breve descrição:

- Registro Eletrônico de Saúde: é uma plataforma digital usada pelos profissionais de saúde para armazenar, gerenciar e compartilhar informações de saúde dos pacientes. Essas informações incluem histórico médico, diagnósticos, tratamentos, medicamentos prescritos, resultados de exames laboratoriais e imagens médicas, dentre outros. Este sistema pode ser acessado por diferentes profissionais de saúde, in-

[4]⟨https://github.com/LucaslcFreitas/Zero-Trust⟩

cluindo médicos, enfermeiros, farmacêuticos e outros membros da equipe médica autorizados.

- Sistema de Informação Hospitalar: é um sistema utilizado em hospitais e clínicas médicas para gerenciar e integrar diversas funções relacionadas à prestação de cuidados de saúde. Esse sistema é composto por vários módulos que podem incluir gestão de recursos humanos, gerenciamento de estoque de medicamentos e materiais, controle financeiro, agendamento de consultas, entre outros.

- Monitoramento Remoto do Paciente: é uma tecnologia que permite que os profissionais de saúde monitorem os pacientes de forma remota, fora do ambiente hospitalar ou clínico tradicional.

- Portal do Paciente: é uma plataforma de tecnologia que permite que os pacientes acessem seus registros médicos eletrônicos, agendem consultas e realizem outras tarefas relacionadas ao seu atendimento de saúde por meio de uma interface online. As informações disponíveis neste sistema podem incluir resultados de exames, histórico médico, listas de medicamentos, informações sobre alergias e outros dados relevantes.

- Telemedicina: é um sistema que permite a realização de consultas e atendimento médico a distância, utilizando tecnologias de comunicação de voz e vídeo. Este sistema normalmente é utilizado para conectar pacientes e profissionais de saúde que estão separados geograficamente, permitindo que pacientes em áreas remotas, por exemplo, tenham acesso a cuidados de saúde que de outra forma não estariam disponíveis.

Além disso, para cada um desses recursos é necessário descrever sua sensibilidade, para compor o controle de acesso juntamente com a confiança atribuída ao usuário.

Classificar a sensibilidade dos recursos é um processo que normalmente requer a opinião de especialistas da área para que se possa quantificar seu risco, porém como o objetivo deste trabalho está na autorização de acesso, às sensibilidades dos recursos foram definidas de forma empírica, atribuindo níveis de sensibilidade a cada recurso com base no

tipo de informação e tipo de ação da requisição. Para a definição das sensibilidade, foram levados em consideração dois pontos principais: o quanto o acesso a um determinado recurso pode impactar na vida ou tratamento dos pacientes e na valiosidade dos dados. A sensibilidade foi classificada no intervalo de 0 a 100, sendo 0 como não sensível e 100 como altamente sensível, conforme Tabelas 4.1, 4.2, 4.3, 4.4 e 4.5.

Sensibilidade: Registro Eletrônico de Saúde				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Informações Cadastrais do Cliente	45	48	68	75
Notas Clínicas	53	80	88	88
Dados de Imunização	38	60	65	65
Histórico Médico	63	95	98	98
Registro de Alergias	43	68	73	73
Resultados Laboratoriais	58	95	98	93
Informações de consentimento	55	95	95	95
Prescrições Médicas	35	60	70	73

Tabela 4.1: Análise de sensibilidade do recurso: Registro Eletrônico de Saúde

Sensibilidade: Sistema de Informação Hospitalar				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Informações Cadastrais do Cliente	45	48	68	75
Registros cadastrais da enfermagem	18	53	63	60
Registros de internação/alta	48	55	70	70
Dados financeiros	48	50	73	73
Dados de recursos humanos	33	53	55	55
Registros de estoque	33	85	85	85

Tabela 4.2: Análise de sensibilidade do recurso: Sistema de Informação Hospitalar

Sensibilidade: Monitoramento Remoto do Paciente				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Registros de sinais vitais	48	60	60	60
Dados de monitoramento de atividades fisicas	23	38	38	38
Dados de geolocalização	43	65	65	65
Dados de análise de tendências	65	-	-	-

Tabela 4.3: Análise de sensibilidade do recurso: Monitoramento Remoto do Paciente

Sensibilidade: Portal do Paciente				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Informações Cadastrais do Cliente	45	48	68	75
Notas Clinicas	53	80	88	88
Informações do plano de saúde	23	-	-	-
Informações de pagamento	38	73	78	78
Informações de consentimento	55	95	95	95

Tabela 4.4: Análise de sensibilidade do recurso: Portal do Paciente

Sensibilidade: Telemedicina				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Informações Cadastrais do Cliente	45	48	68	75
Gravações de consultas	53	73	-	65
Videoconsultas	90			

Tabela 4.5: Análise de sensibilidade do recurso: Telemedicina

4.3 Análise de Confiança

Os mecanismos de avaliação de confiança desempenham um papel fundamental no suporte à tomada de decisões em sistemas de controle de acesso. Eles são utilizados para avaliar o grau de confiança de usuários em potencial, determinando assim a probabilidade de que identidades possam estar comprometidas e poderem realizar ações que possam comprometer a segurança do sistema.

O cálculo de confiança do usuário pode ser realizado de diversas maneiras, tendo como principal fator de avaliação, a análise com base no seu comportamento. Com base neste preceito, a proposta de avaliação de confiança foi realizada a partir de 3 perspectivas, cada uma gerando uma pontuação de 0 a 100:

- Confiança ao usuário baseado no contexto: Nesta fase a confiança é determinada com base na forma como os usuários interagem com o sistema, ou seja, envolve características como o ambiente físico, o momento do dia, a localização geográfica, etc. Neste sentido, os seguintes fatores de penalização foram elaborados:
  - P1: Múltiplos logins falhos consecutivos recentes
  - P2: Alterações de senha recente
  - P3: Mudanças considerável na localização com base nos acessos recentes
  - P4: Acesso fora do horário estipulado (proporcional ao quanto)
  - P5: Redução de privilégios recentes
  - P6: Mudança da rede que utiliza para conectar ao sistema
- Confiança ao dispositivo: Tão importante quanto o contexto, a avaliação do dispositivo utilizado para acesso pode indicar anomalias no acesso. Desta maneira, os seguintes fatores de penalização foram elaborados:
  - P7: Dispositivo nunca utilizado anteriormente
  - P8: Dispositivo compartilhado por outros usuários
  - P9: Alteração nas características do dispositivo (*Device Fingerprint*)
  - P10: Dispositivo com versões de sistema/softwares antigos

- Confiança com base no histórico: Se refere ao nível de confiança ao usuário, com base em seu comportamento passado ao acessar ao um recurso. Isso significa que a confiança do usuário pode ser influenciada pelo histórico de acesso do usuário, incluindo a frequência, a duração e a natureza de suas interações anteriores com o sistema ou serviço. Desta forma, os seguintes fatores foram levados em consideração para o cálculo:

  - P11: Frequência de acesso à recursos altamente sensíveis
  - P12: Múltiplas requisições negadas
  - P13: Usuário recente

Ainda para análise da confiança no histórico, foi levado em consideração a média da confiança das últimas 3 requisições.

Após a análise dos dados mostrados anteriormente, o índice de confiança para a perspectiva de contexto e dispositivo é calculada através da pontuação máxima que ele pode obter (100) subtraindo o somatório das penalidades encontradas, conforme Equação 4.1.

$$C_p = 100 - \left(\sum_{n=1}^{N} A_n \right), \text{ onde } A_n \in [0, 100] \tag{4.1}$$

Onde N é o número de características avaliadas, A_n é a avaliação de penalidade para a característica n e C_p é o resultado da confiança na perspectiva p, numa escada no intervalo $C_p \in [0, 100]$.

Para o cálculo de confiança do histórico, há apenas uma pequena alteração em relação às demais perspectivas, onde ao final é feito uma média com os últimos 3 acessos, conforme Equação 4.2.

$$C_h = \frac{\left(100 - \left(\sum_{n=1}^{N} A_n\right)\right) + M}{2}, \text{ onde } A_n, M \in [0, 100] \tag{4.2}$$

Onde N é o número de características avaliadas, A_n é a avaliação de penalidade para a característica n, M é a média da confiança dos últimos 3 acessos e C_h é o resultado da confiança do histórico.

Por fim, a Equação 4.3 determina o cálculo final da confiança do usuário para a sua requisição.

$$C_u = (\sqrt{C_c \cdot C_d})P, onde P = \begin{cases} \frac{1}{100}C_h, C_h > 0 \\ 0.1, C_h = 0 \end{cases} \quad (4.3)$$

Onde C_h é a confiança com base no histórico, P é normalização do valor de C_h em [0.1, 1], C_d é a confiança com base no dispositivo, C_c é a confiança com base no contexto e C_u é resultado final da confiança do usuário.

Desta forma, a confiança com base no histórico possui uma relevância alta no resultado final, o que contribui para um dos requisitos do *Zero Trust*, onde um usuário recente recebe baixa confiança e privilégios mínimos.

4.4 Banco de Dados

Para armazenamento das configurações e dados gerados na execução do sistema de controle de acesso, foi utilizado o banco de dados relacional PostgreSQL[5]. Além disso, para realizar a conexão entre o ZT e o banco de dados, foi utilizado a biblioteca psicopg2[6].

Na Figura 4.3 temos a modelagem do banco de dados no qual possui 14 entidades, para armazenar informações desde os usuário até os recursos. A tabela *Usuario* é utilizada para armazenar as informações principais de cada usuário. Como neste sistema há diferentes tipos de usuário, foi empregado também sua especialização/generalização em duas tabelas, `Paciente` e `Profissional`, onde na tabela `Profissional` é armazenada as informações dos funcionários.

[5] ⟨https://www.postgresql.org/⟩
[6] ⟨https://pypi.org/project/psycopg2/⟩

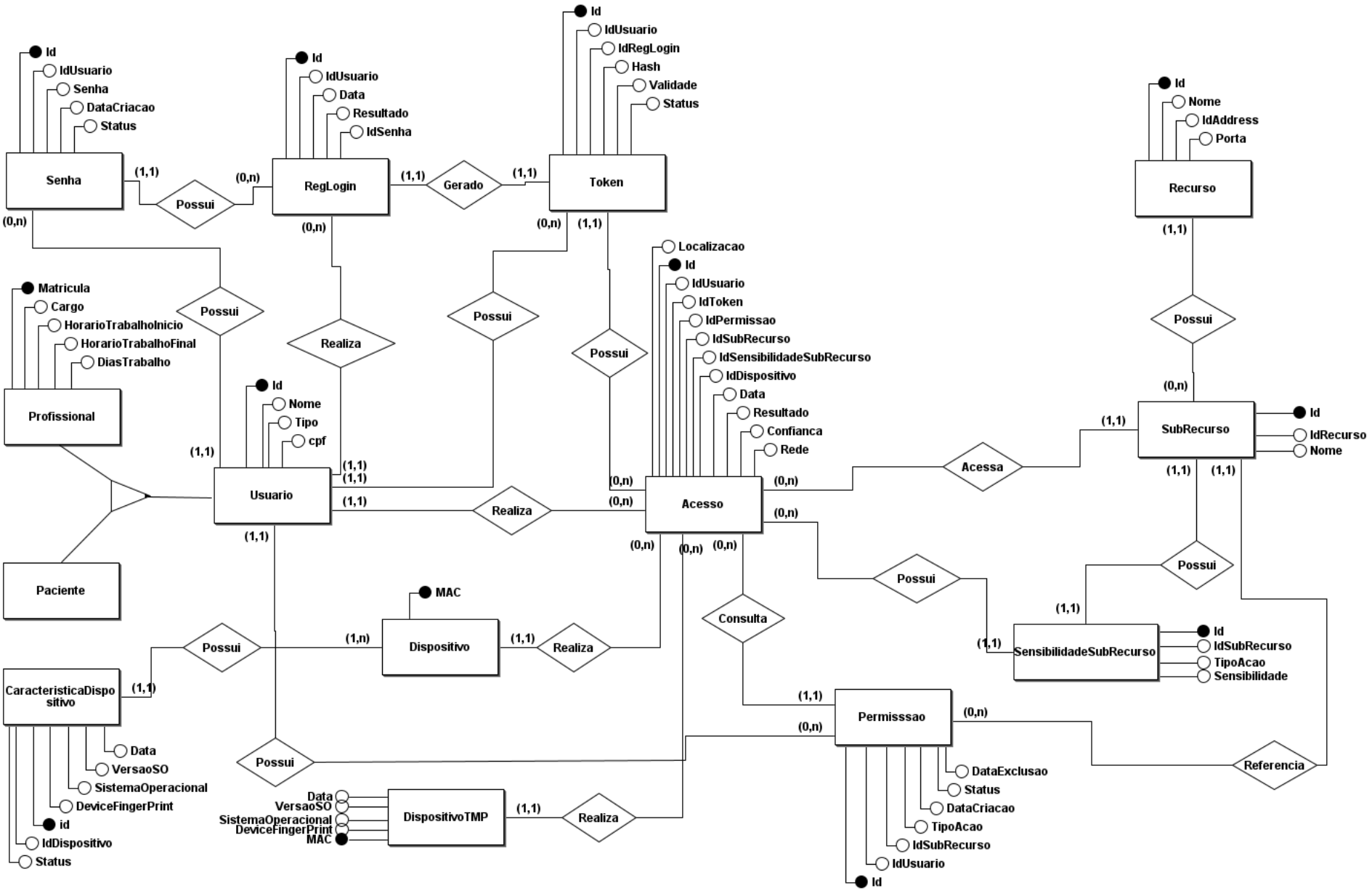


Figura 4.3: Modelagem do banco de dados

Para armazenar as informações referentes a identificação dos usuários, foi utilizados 3 tabelas, além das já citadas: `Senha`, `RegLogin` e `Token`, onde mantém as informações necessárias para autenticação dos usuários, registro de login e também utilizada como parte da análise de confiança no controle de acesso.

Ainda com relação aos usuário, as entidades `Dispositivo` e `CaracteristicaDispositivo` armazenam as informações dos dispositivos utilizados para acesso, do mesmo modo que mantém o histórico de mudanças nas suas características. Além disto, foi utilizado também a tabela auxiliar `DispositivoTMP` para armazenar informações dos dispositivos em acessos negados ou em processo de reautenticação, como forma de não interferir nos dispositivos já registrados em acessos permitidos.

Em relação aos recursos, a tabela `Recursos` armazena os recursos disponíveis e as informações necessárias para conexão (IP e porta), juntamente com a tabela `SubRecurso`, que armazena cada sub-recurso disponível para cada recurso existente. Além disto, a tabela `SensibilidadeSubRecurso` armazena, para cada sub-recurso, sua sensibilidade de acordo com o tipo de ação realizado, conforme discutido na Seção 4.2.

Na tabela `Permissao` são armazenados os registros de quais sub-recursos os usuários naturalmente possuem permissão de acesso, com determinado tipo de ação. Esta informação funciona como primeira verificação de acesso, que será analisada pelo ZT.

Por fim, a tabela `Acesso` é utilizada para armazenar todos os acessos realizados, sendo permitidos, negados ou mediante de reautenticação. Ela se relaciona com a maioria das entidade já citadas anteriormente de forma a poder detalhar todo o processo, como: quem acessou, por qual token, com qual dispositivo, sua localização, o recurso acessado, o tipo de ação realizado, sua rede, o nível de confiança calculado, o horário e o resultado final.

5 Experimentos e Resultados

Neste capítulo é abordado os testes realizados para avaliação do sistema desenvolvido, os cenários definidos, descrevendo seus detalhes e discutindo os resultados obtidos.

Para realização dos testes, foi definido instâncias que definem o comportamento do usuário. Conforme exemplo da Figura 5.1, em cada instância um vetor define uma sequência de operação que um usuário realiza, passando também os dados necessários para acesso, de forma a simular um fluxo de uso. Portanto para realizar uma operação de acesso por exemplo, o usuário deve enviar ao ZT o tipo de operação a realizar, o recurso que deseja acessar, o tipo de ação realizado em cima do recurso, seu token de acesso, a rede utilizada, sua localização, o horário e informações do dispositivo utilizado (*Device Fingerprint*, MAC, sistema operacional e versão). Deste modo foi possível simular todo um contexto de uso, desde a rede até o horário de acesso.


```
[
    {
        "TYPE": "LOGIN",
        "REGISTRY": "460.395.930-32",
        "PASSWORD": "URtrE4lfJ7",
        "IP_ADDRESS": "172.16.10.1/24",
        "LATITUDE": "-21.7866751",
        "LONGITUDE": "-43.3688645",
        "MAC": "CA-14-17-8G-9E-9F",
        "DFP": "29930a0e2ea9e88d47e59571862aaf2c01781cbef7dbac0615e9efe383c8235b",
        "OS": "Windows 10",
        "VERSION_OS": "21H2",
        "TIME": "2023-06-15 13:35:19.047062"
    },
    {
        "REAUTHENTICATE": true,
        "TYPE": "ACCESS",
        "RESOURCE": "Sistema de Informacao Hospitalar",
        "SUB_RESOURCE": "Registros Cadastrais da Enfermagem",
        "TYPE_ACTION": "Leitura",
        "IP_ADDRESS": "172.16.10.1/24",
        "LATITUDE": "-21.7866751",
        "LONGITUDE": "-43.3688584",
        "MAC": "CA-14-17-8G-9E-9F",
        "DFP": "29930a0e2ea9e88d47e59571862aaf2c01781cbef7dbac0615e9efe383c8235b",
        "OS": "Windows 10",
        "VERSION_OS": "21H2",
        "TIME": "2023-06-15 13:36:19.047062"
    }
]
```


Figura 5.1: Instância de exemplo de acesso do usuário

Vale ressaltar também que, em sistemas normalmente classificados como sensíveis

(como e-Health, sistemas financeiros, etc) é comum que haja uma análise prévia do dispositivo, para coleta de informações e garantir maior segurança. No caso deste trabalho, o mesmo foi simulado para envio das informações como sistema operacional, versão e *Device Fingerprint*.

Outro ponto interessante neste modelo é a configuração da variável *"REAUTHENTICATE"*, que define em cada requisição se o usuário deverá realizar a reautenticação ou não, caso seja solicitado. Isto é útil pois possibilita testar cenários de acessos ilícitos onde um infiltrante possui de alguma forma acesso a um dispositivo autenticado ou token, porém não detém das credenciais de identificação.

Para realização dos testes, foi determinado alguns cenários, onde foram avaliados os erros e sucessos no controle de acesso, avaliando tanto se acessos legítimos foram negados indevidamente, quanto se acessos ilegítimos foram permitidos erroneamente.

5.1 Cenário 1: Uso Normal

Neste cenário, o objetivo é simular uma sequência de acesso semelhante a um uso normal do cotidiano. Determinar um uso normal é algo complicado, pois pode variar muito dependendo do perfil do usuário, e para isto foi feito uma aproximação.

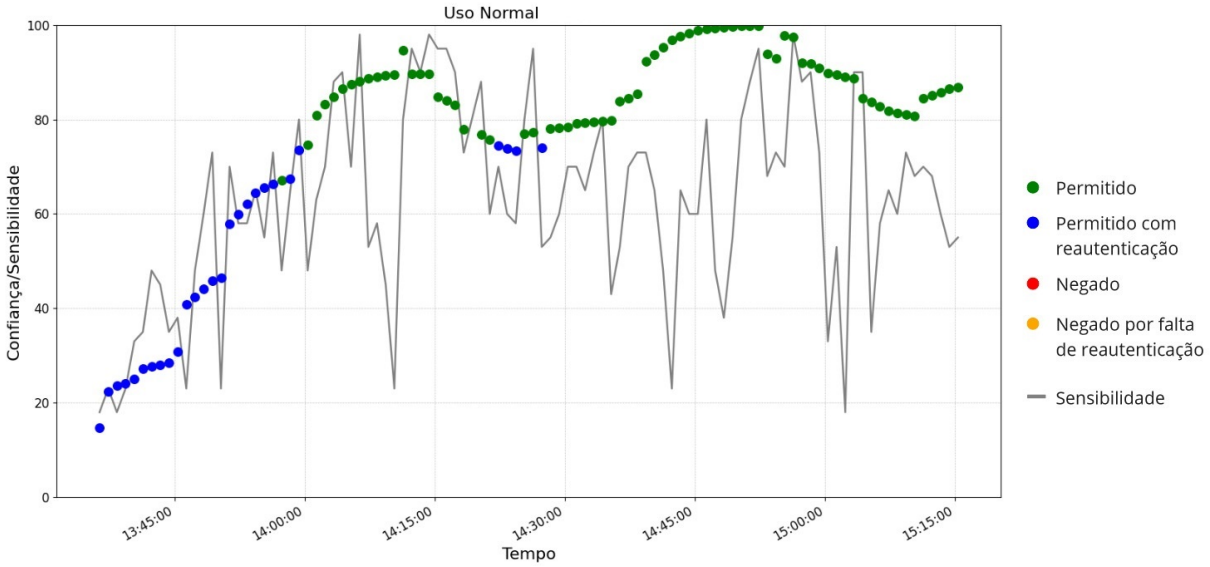


Figura 5.2: Teste cenário 1: Uso Normal

O gráfico 5.2 mostra a simulação realizada com 100 acessos consecutivos, onde

no eixo X temos a confiança/sensibilidade do acesso e no eixo Y o tempo. A linha cinza mostra a sensibilidade do recurso acessado em cada requisição e cada ponto representa um acesso. Os pontos verdes, azuis, vermelhos e laranjas representam os acessos permitidos, permitidos por meio da reautenticação, negado e negado por falta de reautenticação respectivamente.

É possível observar neste primeiro teste que, nas primeiras requisições, o nível de confiança do usuário foi baixo, visto que como se trata de um usuário recente, o sistema não coletou informações suficientes sobre seu comportamento para creditar mais confiança. Portanto nas requisições iniciais o usuário só conseguirá ter acesso aos recursos com sensibilidade mais baixa e por meio de reautenticação, o que está em concordância com a premissa do ZT de definir sempre privilégios mínimos ao usuário.

Podemos observar também que a medida em que o usuário continua a realizar os acessos, sua confiança aumenta gradativamente, até permitir acesso aos recursos com sensibilidade altíssima e não necessitar mais de reautenticação.

Outro ponto interessante a observar é que ao realizar uma sequência de acessos a recursos altamente sensíveis ocorreu um efeito de "onda" reduzindo sua confiança, forçando-o até se reautenticar para continuar o acesso. Isto se deve a penalização P11 da avaliação da confiança com base no histórico, que diz respeito à frequência a recursos altamente sensíveis. Desta forma, esta regra garante uma certa proteção a estes recursos em casos de acessos indevidos.

Para realização dos demais cenários, os mesmos funcionarão como uma sequência deste cenário, cada um com seus casos específicos.

5.2 Cenário 2: Roubo de *Token*

O cenário 2 busca testar casos em que ocorreu a captura de *token* do usuário. Como explicado na Subseção 2.3.2, os *tokens* são utilizados como forma de identificação utilizado após sua devida autenticação, de modo a não exigir que o usuário realize a autenticação a cada acesso.

Testar este caso se faz necessário visto que, com o *token* em mãos, um usuário ilegítimo pode, a princípio, se identificar sem necessariamente possuir as credenciais de

acesso do usuário e permitir acesso a contas, serviços e recursos protegidos, além de realizar ações em nome do usuário sem sua permissão. Desta forma, é imprescindível que o sistema de controle de acesso detecte mudança no uso para identificar e deferir acessos não autorizados.

Existem diversas formas pelo qual um ataque de roubo de *token* pode ocorrer. Dentre as mais conhecidas, uma das formas de obtenção de token é através de interceptação do tráfego de rede, como forma de capturar pacotes na rede (técnica de *sniffing*) ou interceptar e intermediar a comunicação entre entre cliente e servidor (*Man-in-the-Middle*). Outros meios ainda podem ser empregados, como a utilização de *malware* para infectar e capturar *tokens* armazenados nos dispositivos.

Devido às diferentes formas pelo qual este roubo de *token* pode ocorrer, este cenário foi dividido em duas partes: a primeira com acessos em região próxima a de uso do usuário legítimo e o segundo em regiões distantes.

5.2.1 Teste 1: Região Próxima

Para realização deste teste foi considerado que o invasor está localizado em região próxima ao de uso do usuário e não possui as credenciais para autenticação. O fator localização é importante visto que um dos critérios de avaliação da confiança é a avaliação da localização de acesso atual em relação aos acessos anteriores, fazendo com que seja possível detectar mudanças bruscas em um curto intervalo de tempo, ou mesmo avaliar acessos fora dos locais de costume. Além disto, para este teste foi considerado também que para efetuar o acesso, o invasor utilizou outra rede e em um novo dispositivo.

Analisando o gráfico 5.3 podemos perceber que a partir do momento da primeira requisição, foi detectado mudanças no comportamento do usuário e por consequência sua confiança foi reduzida para proteger os recursos. Neste caso, a penalização na confiança ocorreu tanto pela leve alteração de localização, quanto pela mudança repentina de rede e por se conectar com um dispositivo nunca utilizado anteriormente.

Podemos observar também que de imediato, para que o usuário continuasse com o acesso, o sistema exigiu sua reautenticação. Como neste cenário o usuário não dispõe das credenciais de acesso, ele não pode se reautenticar e teve seu acesso negado. Nas

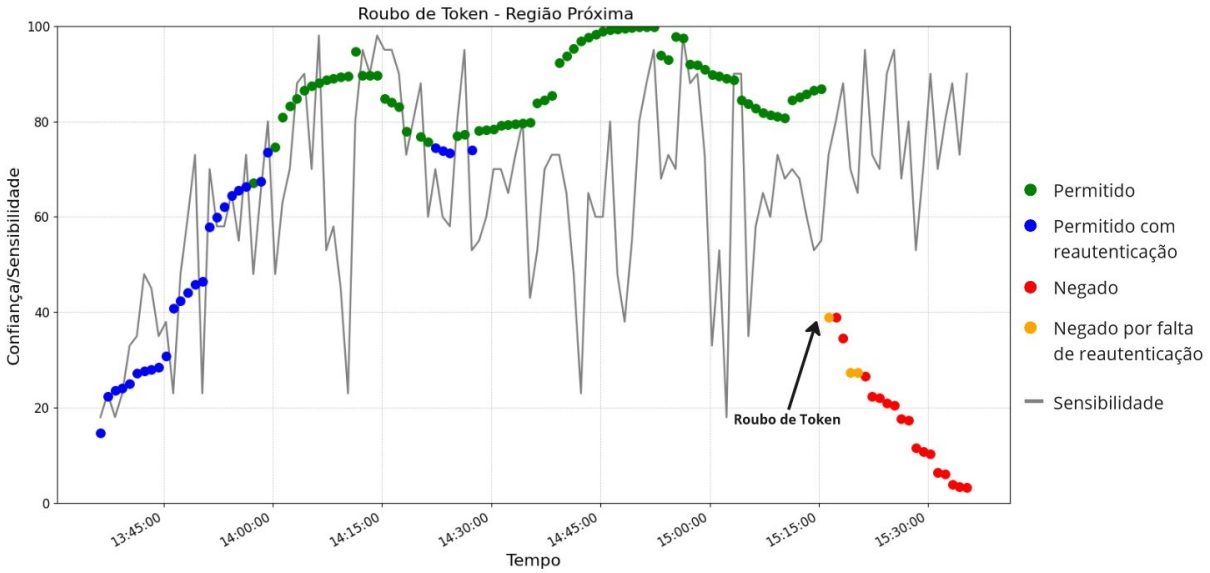


Figura 5.3: Teste cenário 2: Roubo de *token* em região próxima

demais requisições seu acesso foi negado e como decorrência sua confiança foi reduzindo gradativamente.

5.2.2 Teste 2: Região Distante

De forma semelhante ao caso anterior, este teste utilizou as mesmas configurações, porém realizado em uma região muito distante em relação a de uso costumeiro e em um intervalo de tempo muito pequeno. Como podemos observar no gráfico 5.4, neste contexto, como forma de garantir a segurança de seus recursos, todas as requisições foram negadas, não permitindo nem ao menos a possibilidade de reautenticação.

5.3 Cenário 3: Roubo de Credenciais

Neste terceiro cenário, o objetivo é testar a situação de roubo de credenciais de acesso. Este tipo de caso é bastante complexo e complicado de se tomar decisões visto que, como o invasor possui conhecimento das credenciais, o mesmo pode se reautenticar, caso exigido, ficando difícil diferenciar um usuário ilegítimo do legítimo. Portanto, nestas circunstâncias o comportamento do usuário se torna ainda mais relevante para determinar sua confiança.

Para obtenção das credenciais de acesso, um invasor pode utilizar de diversos meios, tendo como principais a utilização de técnicas de engenharia social, onde se faz uso

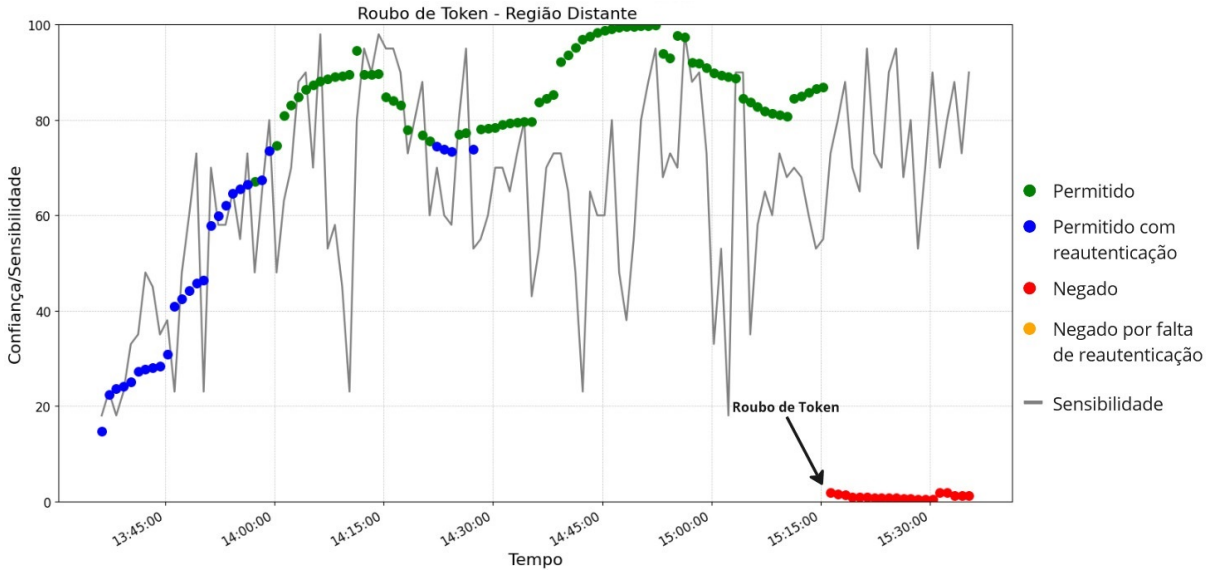


Figura 5.4: Teste cenário 2: Roubo de *token* em região distante

de estratégias para ludibriar o usuário (como e-mails ou mensagens falsas), ou até mesmo com o uso de malwares para captura das teclas digitadas em seu dispositivo, por exemplo (*keylogger*).

Neste sentido, este teste seguiu configurações semelhantes às realizadas no teste 1 do segundo cenário (Subseção 5.2.1), com a diferença de que o invasor possui acesso a credencial e não ao token. Ainda assim, mantendo as tentativas de acesso em uma região próxima ao de acesso do usuário, mas utilizando outra rede e outro dispositivo.

Como podemos observar no gráfico 5.5, neste cenário o sistema proposto apresentou resultados interessantes, porém passíveis de aprimoramento. É possível perceber que o sistema reduziu a confiança ao detectar mudanças em seu comportamento, e dependendo da sensibilidade do recurso requisitado, exigiu a reautenticação ou negou seu acesso. Como o infiltrante possui acesso às credenciais, ele conseguiu acessar alguns recursos de sensibilidade não tão alta, contudo, ainda assim o acesso aos recursos altamente sensíveis foi protegido, tendo neste cenário uma eficiência de 50%.

É possível compreender também neste cenário, que a utilização de um segundo fator de autenticação poderia contribuir para redução dos acessos indevidos, de forma a reduzir a quantidade de informações de identificação que um invasor possa obter.

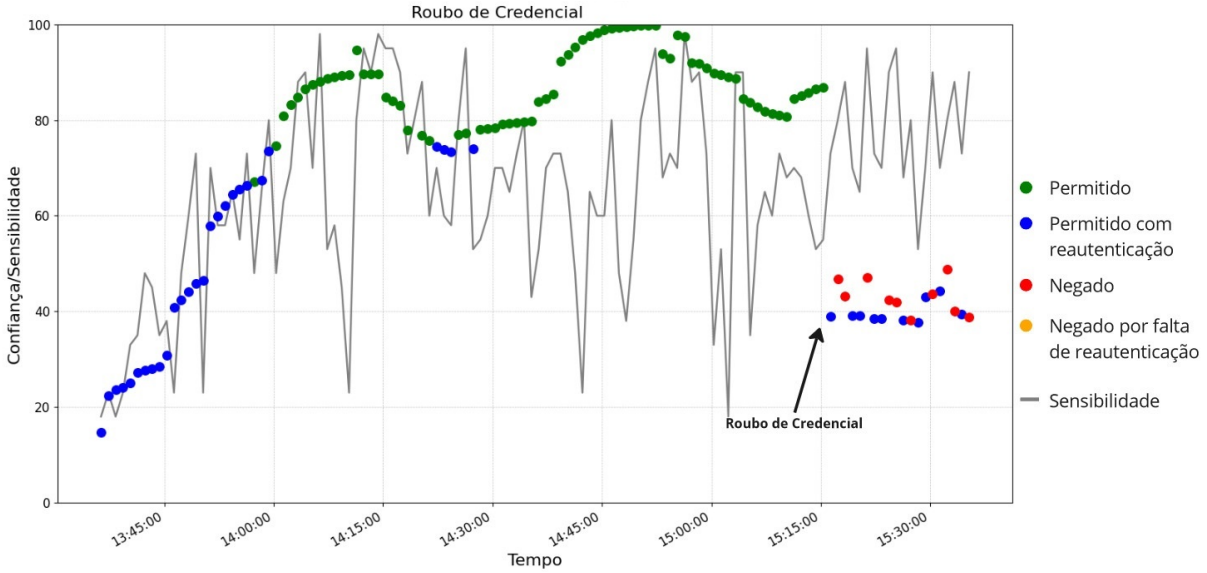


Figura 5.5: Teste cenário 3: Roubo de credencial

5.4 Cenário 4: Ataque de Força Bruta

No quarto cenário, o objetivo foi analisar e testar uma situação de ataque de força bruta. Um ataque de força bruta é uma técnica usada por invasores para tentar quebrar a segurança de uma conta ou sistema ao testar várias combinações possíveis de login em um curto espaço de tempo. Esse tipo de ataque normalmente busca explorar a vulnerabilidade de senhas fracas ou previsíveis, tentando encontrar a combinação correta para obter acesso não autorizado.

Com isso é possível avaliar principalmente como a penalização P1 impacta no controle de acesso. Para isto, este teste foi dividido em duas partes: a primeira sem o sucesso no ataque e o segundo com sucesso.

5.4.1 Teste 1: Sem Sucesso

Neste primeiro caso, foi simulado uma condição onde ocorreu uma série de tentativas de autenticação falhas, enquanto um usuário legítimo realiza seus acessos normais. Testar esta circunstância é importante para mensurar o quanto pode influenciar em um uso regular.

Observando o gráfico 5.6, podemos concluir que este ataque influenciou diretamente no cálculo e queda da confiança do usuário, porém não impediu sua utilização.

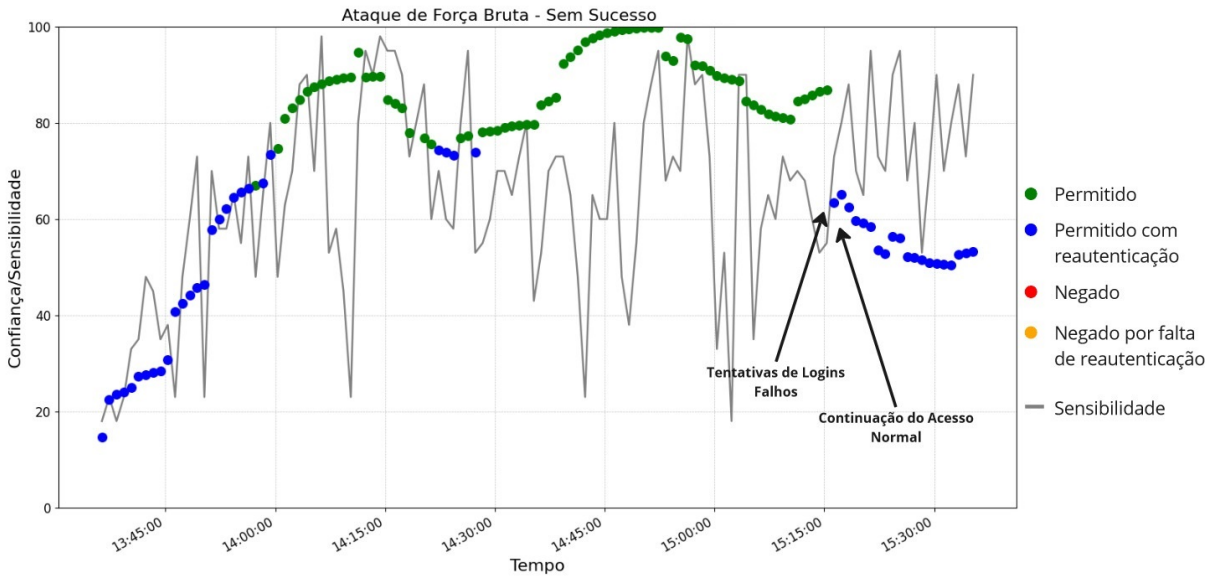


Figura 5.6: Teste cenário 4: Ataque de Força Bruta Sem Sucesso

Como resultado, o sistema protegeu os recursos mais sensíveis exigindo sua reautenticação. É possível observar também que nos últimos acessos sua confiança voltou a crescer, visto que não houve nenhuma outra penalização.

5.4.2 Teste 2: Com Sucesso

Para este segundo teste, foi considerado que após uma sequência de tentativas de login, o invasor conseguiu se autenticar e tentou acessar os recursos. Neste caso foi considerando também que após o sucesso no ataque, o invasor realizou trocas de senhas, uma prática comum para impedir que o usuário legítimo retome o acesso a sua conta.

Além destes fatores, foi definido também que o invasor realizou seus acesso em rede e dispositivo diferente do usuário e em localidade próxima dos acessos anteriores.

É possível perceber pelo gráfico 5.7 que após conseguir se autenticar, devido às diversas tentativas falhas, e as demais configurações deste teste, de imediato a confiança foi drasticamente reduzida, impossibilitando-o de realizar os acessos seguintes, e protegendo em especial, os recursos de sensibilidade média ou superior.

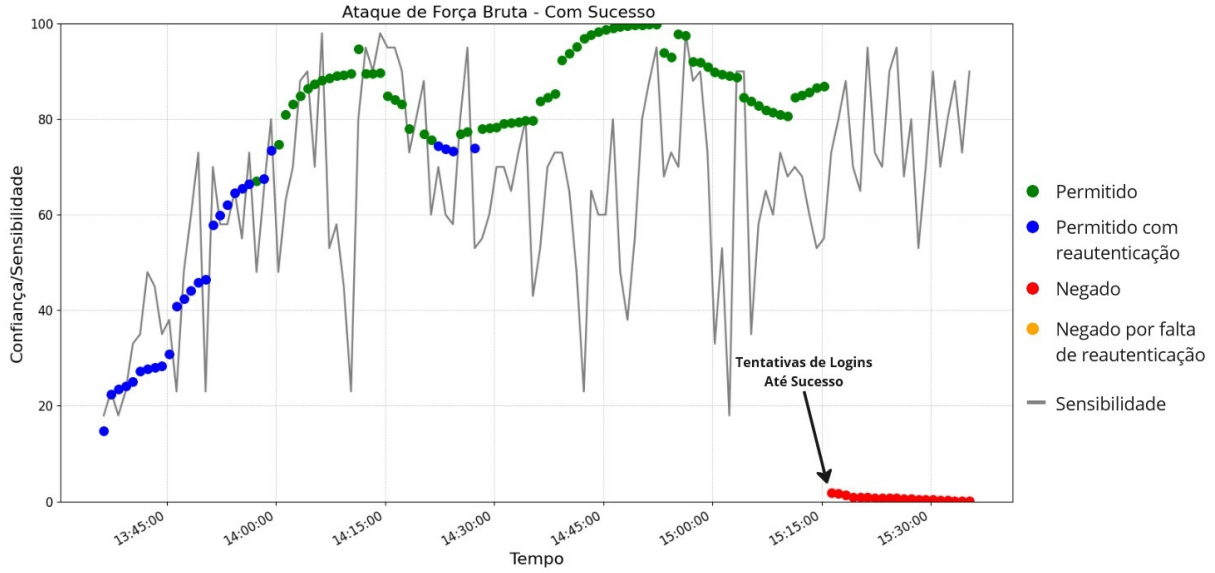


Figura 5.7: Teste cenário 4: Ataque de Força Bruta Com Sucesso

5.5 Cenário 5: Dispositivo Compartilhado

No cenário 5, o objetivo foi testar como o sistema se porta quando um dispositivo é compartilhado por vários usuários. Para isso, após a sequência de acesso normal (mostrado anteriormente), foram realizados alguns acessos por outros 3 usuários no mesmo dispositivo, e em seguida continuou-se os acessos do primeiro usuário.

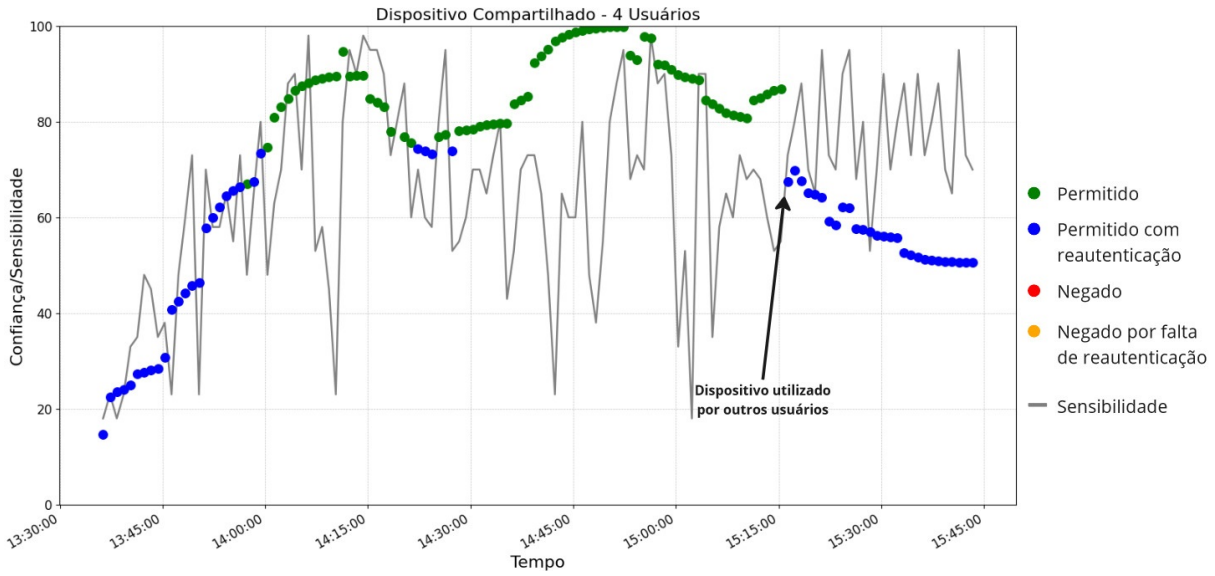


Figura 5.8: Teste cenário 5: Dispositivo Compartilhado

O compartilhamento de dispositivos não necessariamente é uma situação preocupante, porém pode trazer um risco maior à identidade, visto que é mais difícil garantir

que todas as contas estejam protegidas adequadamente. Nestes casos pode acontecer, por exemplo, o esquecimento de contas logadas durante a troca de usuários.

No gráfico da Figura 5.8 temos a visão do primeiro usuário. Podemos observar que, a partir do momento em que é detectado o compartilhamento do dispositivo, a confiança foi reduzida de modo que há a necessidade de reautenticação para realizar o acesso aos recursos altamente sensíveis. Vale ressaltar que neste teste foram feitos 10 acessos a mais que os demais para demonstrar também que, após um período, a redução da confiança se estabiliza em determinado nível (aproximadamente em 55).

5.6 Cenário 6: Acesso Fora do Horário Estipulado

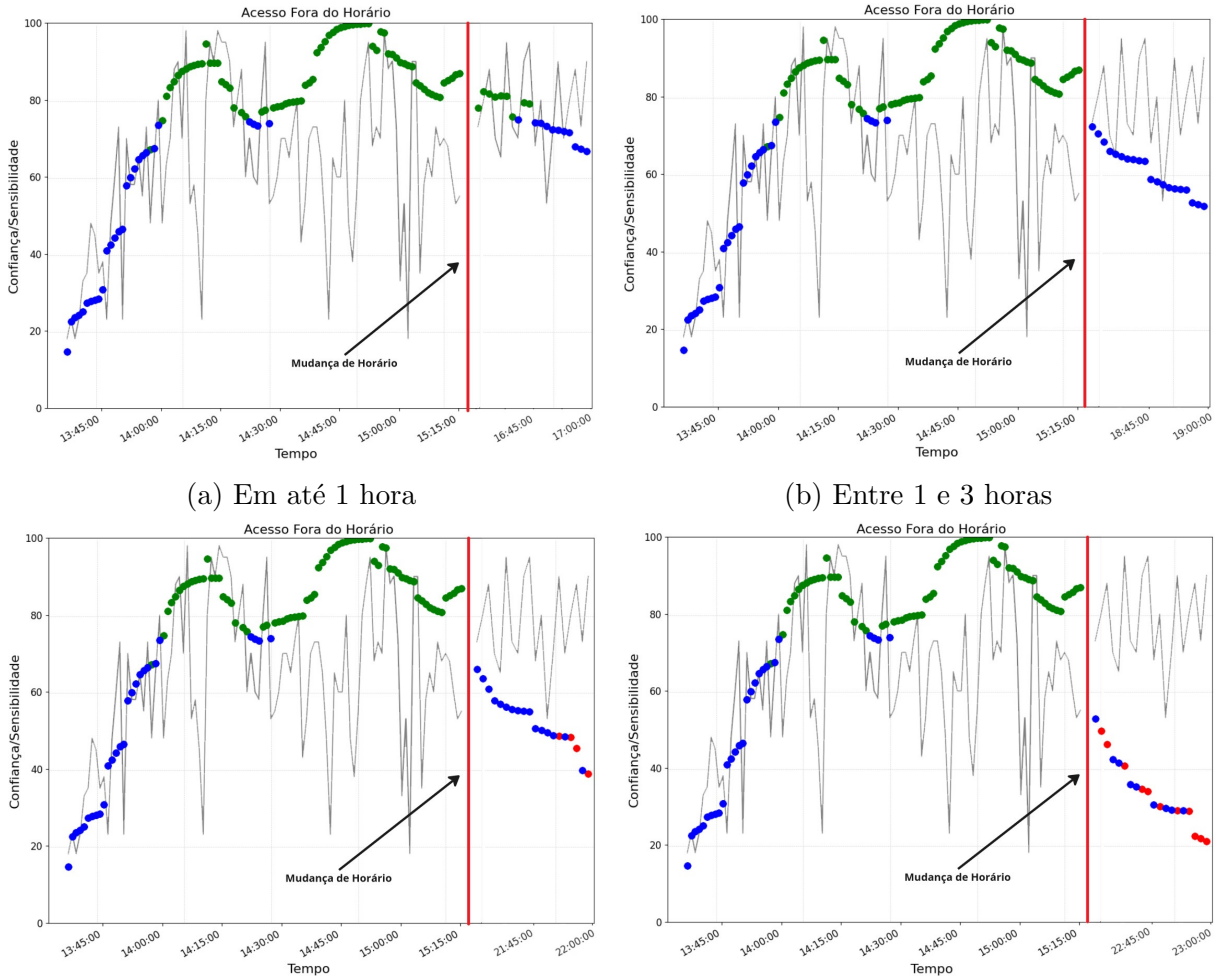
Por fim, no cenário 6 é analisado como o horário de acesso afeta a confiança do usuário. Este cenário se aplica diretamente aos funcionários, que possuem uma carga horária definida de trabalho, e por este meio, é possível determinar se o acesso está dentro dos horários permitidos. Conforme discutido na seção 4.4, para cada usuário foi definido um período e dias de trabalho.

Em um ambiente hospitalar é possível que eventualmente funcionários precisem extrapolar seus horários de trabalho para atender a demanda. Neste sentido, avaliar o horário no controle de acesso de forma mais flexível é importante, tanto para não negar um acesso de um funcionário que precisou extrapolar sua carga horária, quanto para não permitir acessos que estão completamente fora dos horários definidos.

Desta maneira, para a realização da penalização por horário, foi definido primeiramente intervalos do quanto o usuário pode estar fora do horário estipulado, e de acordo com cada faixa, penalizações foram aplicadas de forma gradual.

Portanto, para realização deste cenário, foram realizados testes de um funcionário que trabalha no horário de 08:00 às 16:00 e precisou realizar acessos após o horário definido. Para isso foram definidos 4 testes: com acessos de até 1 hora após seu horário, entre 1 e 3 horas, entre 3 e 6 horas, e superior a 6 horas. Todos os testes como sucessão do cenário 1, com as mesmas configurações, a exceção do horário.

Nos gráficos da Figura 5.9, temos os quatro testes realizados, onde a linha vermelha vertical representa a mudança no tempo de acesso. Sendo assim, os acessos realizados



(a) Em até 1 hora

(b) Entre 1 e 3 horas

(c) Entre 3 e 6 horas

(d) Superior a 6 horas

Figura 5.9: Teste cenário 6: Acesso Fora do Horário Estipulado

antes desta linha vermelha são os acessos normais já mostrados na Seção 5.1 e os posteriores são os acessos realizados em suas respectivos horários.

Como podemos observar nos testes, é possível notar que quando se realiza acessos fora do horário definido, há uma queda na confiança e a intensidade desta queda varia de acordo com o quão fora está do horário limite. Com acessos em até uma hora fora do horário definido (gráfico 5.9a), ocorreu uma leve queda, em que não impediu seu uso, mas já exigiu a reautenticação para acesso aos recursos altamente sensíveis. Já nos acessos que ocorreram entre 1 e 3 horas fora do horário definido(gráfico 5.9b), ocorreu uma queda maior na confiança fazendo com que os recursos com sensibilidade alta ou altíssima só sejam acessíveis mediante reautenticação. Nos acessos que ocorreram entre 3 e 6 horas fora do horário definido (gráfico 5.9c) a queda na confiança foi ainda maior, fazendo com que algumas requisições aos recursos altamente sensíveis fossem negadas, a medida com

que o usuário insiste em realizar seus acessos. Por fim, nos acessos que ocorreram a mais de 6 horas do horário definido, a queda na confiança foi bem mais acentuada, negando boa parte das requisições e oferecendo uma segurança maior aos recursos.

6 Conclusões e Trabalhos Futuros

O presente trabalho demonstrou a implementação de um sistema *Zero Trust* para controle de acesso de usuários em um ambiente de *e-health*, através da análise contínua da confiança, atribuição de privilégios mínimos e do mapeamento das sensibilidade dos recursos. A adoção desse modelo proporcionou uma boa proteção aos recursos, garantindo a confidencialidade e integridade dos recursos.

Através dos variados experimentos realizados, foi possível observar a capacidade de detectar e responder rapidamente a tentativas de acesso ilegítimo. O monitoramento constante dos acessos e a análise comportamental dos usuários permitiram identificar anomalias e atividades suspeitas em tempo real, minimizando assim o impacto de possíveis ataques.

Como resultados, o sistema demonstrou uma eficiente proteção, sobretudo aos recursos de sensibilidade mais elevada e, por consequência, a segurança e a privacidade dos pacientes e profissionais envolvidos.

Como trabalhos futuros, há duas áreas importantes a serem exploradas para aprimorar o sistema *Zero Trust* no ambiente de *e-health*. Primeiramente, é recomendado considerar a implementação de autenticação por segundo fator como uma medida adicional de segurança. Essa abordagem reduziria significativamente o risco de roubo de credenciais (Cenário 3), adicionando uma camada extra de proteção. Ao exigir que os usuários autentiquem-se não apenas com suas credenciais primárias, mas também com um segundo fator, como um código único enviado por SMS ou gerado por um aplicativo, a segurança das informações sensíveis seria fortalecida.

Além disso, é fundamental buscar melhorias na usabilidade do sistema. Embora a autenticação seja uma prática de segurança importante, pode causar inconveniência para os usuários, ao exigir reautenticações frequentes. Nesse sentido, trabalhos futuros podem se concentrar em explorar abordagens que reduzam essa necessidade, sem comprometer a segurança.

Outro ponto a ser considerado é a construção de um portal de administração

dedicado. Esse portal permitiria aos administradores ajustar e personalizar facilmente as políticas de acesso, conceder ou revogar permissões de forma intuitiva, além de fornecer uma visão abrangente das configurações de controle de acesso e métricas de segurança. Com um portal de administração, seria possível gerenciar de maneira eficiente as permissões dos usuários e monitorar as atividades, facilitando a identificação de possíveis anomalias ou tentativas de acesso não autorizado.

Ainda assim, apesar dos trabalhos futuros recomendados para o aprimoramento do modelo, o mesmo se apresentou muito eficaz dentro da sua proposta, podendo ser inclusive, facilmente e implementável em outros segmentos, de acordo com suas necessidades.

Bibliografia

ALACA, F.; OORSCHOT, P. C. V. Device fingerprinting for augmenting web authentication: classification and analysis of methods. In: *Proceedings of the 32nd annual conference on computer security applications*. [S.l.: s.n.], 2016. p. 289–301.

ALI, B.; GREGORY, M. A.; LI, S. Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In: IEEE. *2021 31st international telecommunication networks and applications conference (itnac)*. [S.l.], 2021. p. 192–197.

ATLAM, H.; ALENEZI, A.; WALTERS, R.; WILLS, G. et al. An overview of risk estimation techniques in risk-based access control for the internet of things. INSTICC, 2017.

AWAN, S. M.; AZAD, M. A.; ARSHAD, J.; WAHEED, U.; SHARIF, T. A blockchain-inspired attribute-based zero-trust access control model for iot. *Information*, MDPI, v. 14, n. 2, p. 129, 2023.

BARRA, D. C. C.; NASCIMENTO, E. R. P. do; MARTINS, J. de J.; ALBUQUERQUE, G. L.; ERDMANN, A. L. Evolução histórica e impacto da tecnologia na área da saúde e da enfermagem. *Revista Eletrônica de Enfermagem*, v. 8, n. 3, 2006.

BHATTACHARYYA, D.; RANJAN, R.; ALISHEROV, F.; CHOI, M. et al. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, v. 2, n. 3, p. 13–28, 2009.

COVENTRY, L.; BRANLEY, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, Elsevier, v. 113, p. 48–52, 2018.

CREMONEZI, B.; VIEIRA, A.; NACIF, J.; SILVA, E. F.; NOGUEIRA, M. Um método para extração e refinamento de políticas de acesso baseado em árvore de decisão e algoritmo genético. In: SBC. *Anais do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. [S.l.], 2021. p. 686–699.

DHARAVATH, K.; TALUKDAR, F. A.; LASKAR, R. H. Study on biometric authentication systems, challenges and future trends: A review. In: IEEE. *2013 IEEE International Conference on Computational Intelligence and Computing Research*. [S.l.], 2013. p. 1–7.

DIAS, F. M. et al. Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saúde. Universidade Nove de Julho, 2021.

D'SILVA, D.; AMBAWADE, D. D. Building a zero trust architecture using kubernetes. In: IEEE. *2021 6th international conference for convergence in technology (i2ct)*. [S.l.], 2021. p. 1–8.

GUERRA, E. M.; PAIVA, R. C. de; FERNANDES, C. T. Rbac com contextos: modelo de controle de acesso baseado em papéis para sistemas web utilizados por várias divisões de uma organização. *6º Simpósio Segurança em Informática, São José dos Campos, São Paulo, Brasil*, 2004.

HU, V. C.; KUHN, D. R.; FERRAIOLO, D. F.; VOAS, J. Attribute-based access control. *Computer*, IEEE, v. 48, n. 2, p. 85–88, 2015.

JAIN, A. K.; NANDAKUMAR, K. Biometric authentication: System security and user privacy. *Computer*, v. 45, n. 11, p. 87–92, 2012.

KIM, H.; KIM, D.-K.; ALAERJAN, A. Abac-based security model for dds. *IEEE Transactions on Dependable and Secure Computing*, IEEE, 2021.

LAL, N. A.; PRASAD, S.; FARIK, M. A review of authentication methods. *vol*, v. 5, p. 246–249, 2016.

LEANDRO, M. A. P. et al. Federação de identidades e computação em nuvem: estudo de caso usando shibboleth. Florianópolis, 2012.

LI, J.; BAI, Y.; ZAMAN, N. A fuzzy modeling approach for risk-based access control in ehealth cloud. In: IEEE. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. [S.l.], 2013. p. 17–23.

LIAO, I.-E.; LEE, C.-C.; HWANG, M.-S. A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, Elsevier, v. 72, n. 4, p. 727–740, 2006.

LUH, F.; YEN, Y. Cybersecurity in science and medicine: Threats and challenges. *Trends in biotechnology*, Elsevier, v. 38, n. 8, p. 825–828, 2020.

MAIA, G. *Saúde foi o setor mais afetado por tentativas de ciberataques, diz ISH*. 2021. Disponível em: ⟨https://veja.abril.com.br/coluna/radar/saude-foi-o-setor-mais-afetado-por-tentativas-de-ciberataques-diz-ish/⟩.

MIZRACHI, A. *Understanding Token-Based Authentication: A Detailed Review*. 2021. Disponível em: ⟨https://frontegg.com/blog/token-based-authentication⟩.

OBELHEIRO, R. R.; FRAGA, J.; WESTPHALL, C. M. Controle de acesso baseado em papéis para o modelo corba de segurança. In: *Proc. 19th Brazilian Symp. Comp. Networks*. [S.l.: s.n.], 2001.

ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. *Zero trust architecture*. [S.l.], 2020.

SANTOS, D. R. d. et al. Uma arquitetura de controle de acesso dinâmico baseado em risco para computação em nuvem. 2013.

SANTOS, D. R. D.; WESTPHALL, C. M.; WESTPHALL, C. B. A dynamic risk-based access control architecture for cloud computing. In: IEEE. *2014 IEEE Network Operations and Management Symposium (NOMS)*. [S.l.], 2014. p. 1–9.

SHARMA, A.; SHARMA, S.; DAVE, M. Identity and access management-a comprehensive study. In: IEEE. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. [S.l.], 2015. p. 1481–1485.

SHEN, H.-b.; HONG, F. An attribute-based access control model for web services. In: IEEE. *2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)*. [S.l.], 2006. p. 74–79.

SOUZA, W. S. d. *Superando os riscos da segurança baseada em perímetro-Uma abordagem com identificação federada através de certificados digitais A3/ICP-Brasil e SAML*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, 2013.

TEERAKANOK, S.; UEHARA, T.; INOMATA, A. Migrating to zero trust architecture: reviews and challenges. *Security and Communication Networks*, Hindawi, v. 2021, 2021.

TORTELLA, T. *Após 13 dias fora do ar, ConecteSUS volta a funcionar, diz Ministério da Saúde*. 2021. Disponível em: ⟨https://www.cnnbrasil.com.br/saude/apos-13-dias-fora-do-ar-conectesus-volta-a-funcionar-diz-ministerio-da-saude/⟩.

TYLER, D.; VIANA, T. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Applied Sciences*, MDPI, v. 11, n. 16, p. 7499, 2021.

UEDA, E. T. *Análise de políticas de controle de acesso baseado em papéis com rede de Petri colorida.* Tese (Doutorado) — Universidade de São Paulo, 2012.

XU, Q.; ZHENG, R.; SAAD, W.; HAN, Z. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, IEEE, v. 18, n. 1, p. 94–104, 2015.

ZEADALLY, S.; ISAAC, J. T.; BAIG, Z. Security attacks and solutions in electronic health (e-health) systems. *Journal of medical systems*, Springer, v. 40, p. 1–12, 2016.