UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE ESTATÍSTICA E INFORMÁTICA
CIÊNCIA DA COMPUTAÇÃO

VICTOR ALEXANDRE DE OLIVEIRA SILVA

Uma Metodologia para Modelagem de Ameaças em Ambientes Baseados na Internet das Coisas

Recife
2018

VICTOR ALEXANDRE DE OLIVEIRA SILVA

Uma Metodologia para Modelagem de Ameaças em Ambientes Baseados na Internet das Coisas

Monografia apresentada ao curso de Ciência da Computação, como parte dos requisitos necessários à obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Fernando Antonio Aires Lins

Recife

2018

MINISTÉRIO DA EDUCAÇÃO E DO DESPORTO
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

http://www.bcc.ufrpe.br

Anexo E
PARECER DE AVALIAÇÃO DAS CORREÇÕES DO TRABALHO DE CONCLUSÃO DE CURSO

Dados do Trabalho	
Orientador	Fernando Antônio Aires Lins
Co-orientador	-
Aluno	Victor Alexandre de Oliveira Silva
Título	Uma Metodologia para Modelagem de Ameaças de Segurança em Ambientes Baseados na Internet das Coisas
Número da Defesa	057

Em análise às correções solicitadas como requisito para finalização do Trabalho de Conclusão de Curso, atesto que as mesmas foram **cumpridas**.

Recife, 01 de Março de 2018

Fernando Antônio Aires Lins

Dedico este trabalho à memória de Chester Charles Bennington, a quem agradeço, sobretudo, por ser a minha voz durante toda a minha vida.

Agradecimentos

A Deus pelo direcionamento, força e sabedoria para concluir este curso.

À minha mãe, Sônia, por desde sempre me mostrar o valor do conhecimento. Também agradeço por todo os sacrifícios feitos para que obtivesse o máximo de educação possível.

À Natália por ser, acima tudo, uma parceira para a vida.

Ao meu professor e orientador, Fernando Aires, pela paciência, calma e disponibilidade ao me conduzir no desenvolvimento deste trabalho.

Ao *City College University of New York - College of Staten Island* pelo acolhimento e por me ressuscitar academicamente durante o período de intercâmbio. Em especial, a todos os amigos e laços formados durante o período de intercâmbio. Por conta deles, carrego um pedaço de cada canto do mundo dentro de mim.

A todos os amigos e companheiros de caminhada pelos sorrisos e momentos de descontração, os quais foram fundamentais durante este período de tamanha sobrecarga.

Ao Victor de 4 anos atrás por não ter desistido de mim e por ter acreditado em sonhos impossíveis até então.

À banda Linkin Park, por ser minha companhia nos momentos em que a solidão chegou a ser palpável; por ser minha voz nas vezes em que a vida tirou a minha; por ser a luz que iluminou a caminhada tantas vezes obscura; por ser a mão estendida em meu auxílio; por partilhar meus sorrisos e momentos de alegria; por ser a trilha sonora mais perfeita da vida; por formar e ser parte de quem eu sou. À esta banda, minha imensurável gratidão.

Resumo

A Internet das Coisas tem surgido como um paradigma emergente e de considerável expansão. Com a proposta de interconexão entre pessoas, coisas e serviços em qualquer lugar e a qualquer momento, a Internet das Coisas tem permitido o desenvolvimento de aplicações em diversas áreas como ambientes inteligentes, *healthcare*, transporte e aplicações pessoais. Tais aplicações poderão ter impacto direto na forma como vivemos, trabalhos e interagimos. Contudo, a interconexão de bilhões de novos dispositivos à rede e a alta interoperabilidade de tecnologias pode aumentar potencialmente a superfície de ataque da Internet como um todo, o que pode conduzir ao aumento de riscos de segurança. Uma maior superfície de ataque implica diretamente em mais oportunidades para atacantes que desejem realizar atividades maliciosas em sistemas baseados na Internet das Coisas. Consequentemente, novas técnicas, metodologias e soluções necessitam ser desenvolvidas para o tratamento das questões de segurança em IoT. Neste sentido, este trabalho propõe uma metodologia de modelagem de ameaças aplicável à Internet das Coisas. Através da revisão da literatura, foi possível identificar e analisar as principais metodologias existentes para contextos generalistas, que se aplicam a qualquer tipo de sistema, e trabalhos com propostas iniciais de modelagem de ameaças específicos para ambientes de Internet das Coisas. A partir desta revisão e análise da literatura, foi possível desenvolver uma metodologia base, a qual foi finalmente refinada e adaptada para a Internet das Coisas. A metodologia proposta visa auxiliar no processo de identificação, categorização e classificação de ameaças em ambientes baseados na Internet das Coisas. Desta forma, espera-se auxiliar no processo de avaliação do estado de segurança de sistemas IoT, na extração de requisitos de segurança, no auxílio à priorização de esforços de segurança e no apoio à fase de desenvolvimento e projeto seguro de sistemas inseridos no contexto da Internet das Coisas. O presente trabalho define e explana as principais etapas e atividades do processo de modelagem de ameaças proposto, assim como o aplica em um estudo de caso, com o intuito de ilustrar e avaliar a sua aplicação em um cenário real.

Palavras-chave: Internet das Coisas, segurança da informação, modelagem, ameaça, risco.

Abstract

The Internet of Things has emerged as a fast-growing paradigm. Proposing high interconnection between people, things and services, anywhere and at any time, the Internet of Things has allowed the development of applications in several areas such as smart environments, healthcare, transportation and personal applications. Such applications can have direct impact on how we live, work and interact. However, the interconnection of billions of new devices to the network and the high interoperability of technologies can potentially increase the attack surface of the Internet as a whole, which can lead to the increase of security risks. A wide attack surface means more opportunities for attackers who wish to perform malicious activities on systems based on the Internet of Things. Consequently, new techniques, methodologies and solutions need to be developed for the treatment of security issues in IoT considering its own properties. For this reason, this work proposes a threat modeling methodology applicable to the Internet of Things. Through the literature review, it was possible to identify and analyze the current methodologies proposed for generalist contexts, which can be applied on any system, and initial proposed works for threat modeling in IoT systems. From the review and analysis of the literature, it was possible to develop a inital methodology, which was finally refined and adapted to IoT. The present work defines and explains the main steps and activities of the proposed process, as well as applies it in an evaluation environment used as a case study. The purpose of this methodology is to assist in the identification, categorization and classification of threats in environments based on the Internet of Things. In this way, it aims to help in the process of evaluating the security state of IoT systems, to extract security requirements, to assist the prioritization of security efforts and to support the development phase and secure design of systems inserted in the context of Internet of Things.

Keywords: Internet of Things, information security, modeling, threat, risk

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

API	Application Programming Interface
BPMN	Business Process Modeling Notation
DFD	Diagrama de Fluxo de Dados
GPS	Global Position System (USA)
HTTP	Hyper Text Transport Protocol
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
NFC	Near Field Communication
REST	Representational State Transfer
RFID	Radio-Frequency IDentification (identificador por radiofrequência)
SDK	Software Development Kit
STRIDE	Spoofing, Tampering, Repudiation, Informarion Disclosure, Denial of Service, Elevation of Privilege
TCP/IP	Transmission Control Protocol/Internet Protocol
UML	Linguagem de Modelagem Unificada (do inglês, Unified Modeling Language)

Sumário

1 Introdução

1.1 Contexto

Desde a sua concepção, a Internet permanece evoluindo e se adaptando aos novos requisitos exigidos pelas novas tendências de mercado, pelas mudanças da sociedade ou pela sua própria reestruturação arquitetural. Nos dias atuais, a Internet das Coisas tem se tornado o próximo passo na evolução da Internet(JADOUL, 2015) .

A Internet das Coisas (do inglês *Internet of Things*) pode ser entendida através de diversas perspectivas. Em uma de suas definições, a IoT apresenta-se como a interconexão de dispositivos físicos, compostos por softwares, sensores, atuadores e eletrônicos, que possuem conectividade à Internet, permitindo que estes dispositivos coletem e troquem dados entre si(SAIN; KANG; LEE, 2017). Estes dispositivos, por sua vez, também se utilizam de interfaces inteligentes e são conectados de forma transparente à uma infraestrutura global e dinâmica de rede com característica autoconfigurável, baseada em padrões e que possui protocolos interoperáveis de comunicação(EUROPEAN RESEARH CLUSTER ON INTERNET OF THINGS, 2015).

O surgimento, evolução e adoção da Internet das Coisas tem permitido o desenvolvimento de novas aplicações que terão impactos significativos em diversas áreas da sociedade.Em um estudo realizado pela Gartner (2013), é previsto que em 2020 o número de dispositivos IoT conectados à Internet seja de 26 bilhões de ativos, evidenciando a importância e a grande expectativa de expansão da Internet das Coisas. Dentre as principais áreas de aplicação da Internet das Coisas, podemos citar ambientes inteligentes, aplicações na indústria de *healthcare*, no seguimento de logística, transporte, aplicações pessoais e sociais(ATZORI; IERA; MORABITO, 2010).

Ambientes baseados na Internet das Coisas são constituídos, em sua maioria, por dispositivos que possuem restrições energéticas, de processamento e de armazenamento. Ainda, tais dispositivos são facilmente acessíveis fisicamente e utilizam tecnologias baseadas em redes sem fio para comunicação. Tais características, dentre outras, cooperam para a introdução de diversos desafios no domínio da segurança da informação no âmbito da Internet das Coisas.

Dentre os principais desafios de segurança da informação, podemos destacar a identificação única e global de objetos, mecanismos de autenticação, autorização e garantia de privacidade, protocolos de comunicação seguros, sistemas de criptografia adequados, contramedidas aos ataques mais comuns a dispositivos IoT, dentre outros (ABOMHARA; KØIEN, 2014; ZHANG et al., 2014).

Os desafios de segurança da informação em IoT mostram que seus aspectos de segurança necessitam ser tratados considerando as características deste contexto. Isto implica dizer que a escolha dos mecanismos de segurança a serem implantados em ambientes baseados na Internet das Coisas necessitam ser escolhidos levando em consideração as restrições e requisitos exigidos por este paradigma. Desta forma, torna-se clara a necessidade da proposição de novas técnicas e/ou metodologias que visem tratar os desafios de segurança impostos pela Internet das Coisas e auxiliar no processo de proposição de mecanismos e soluções de segurança aplicáveis à Internet das Coisas.

Trabalhos como (COVINGTON; CARSKADDEN, 2016; NAWIR; AMIR; YAAKOB, 2013; GUBBI et al., 2013) evidenciam a relevância do tratamento das questões de segurança para IoT através de estudos que propõem, por exemplo, a identificação de desafios de segurança para IoT, o mapeamento da taxonomia de ataques para IoT, *frameworks* e guias de segurança, dentre outras contribuições.

Além das iniciativas para tratar de segurança em IoT, técnicas tradicionais de segurança previamente estabelecidas e utilizadas por outras áreas da computação também podem ser utilizadas como base para a proposição de soluções voltadas à Internet das Coisas (SÁNDOR; SEBESTYÉN-PÁL, 2017).

O processo de modelagem de ameaças foi primeiramente introduzido pela Microsoft. Em sua proposta inicial (MICROSOFT, 2003), a modelagem de ameaças foi introduzida na etapa de *design* do SDL (*Secure* Development *L*ifecycle) de aplicações de software apresentada pela companhia. Como ideia central, o processo de modelagem de ameaças visa prover uma metodologia sistemática para a identificação, categorização e classificação de ameaças de segurança associadas a um objetivo de análise. Como benefícios e vantagens da utilização de modelagem de ameaças, pode-se destacar: a abordagem sistemática de identificação de ameaças associadas a um determinado sistema, a categorização e classificação das ameaças identificadas, a identificação mais efetiva de contramedidas de segurança baseada nas ameaças identificadas, insumos concretos para justificar os esforços de segurança, o auxílio na fase de design do sistema sob construção, extração de requisitos de segurança a partir do modelo de ameaça gerado, dentre outros.

Trabalhos como (CHOWDHURY; MACKENZIE, 2014; WANG; ALI; KELLY, 2015; SÁNDOR; SEBESTYÉN-PÁL, 2017) apresentam propostas iniciais para modelagem de ameaças em sistemas da Internet das Coisas. Contudo, tais trabalhos focam-se em contextos de aplicações específicas da Internet das Coisas. Tais limitações dificultam a reutilização das metodologias e abordagem desses trabalhos para a realização de modelagem de ameaças em outros contextos da Internet das Coisas.

Neste sentido, o presente trabalho visa a proposição de uma metodologia de

modelagem de ameaças de segurança adaptada a ambientes baseados na Internet das Coisas, buscando utilizar os conceitos e migrar os benefícios desta técnica para o contexto de IoT.

1.2 Problema e Justificativa

As questões e desafios de segurança constituem uma área de relevância no contexto da Internet das Coisas. De acordo com Atamli e Martin (2014) o não tratamento dos requisitos de segurança e privacidade podem comprometer a ampla adoção deste paradigma. Trabalhos como (IRSHAD, 2016) demonstram a potencial gravidade que as consequências da exploração de falhas de segurança em sistemas IoT podem ter em diversos ramos de aplicação, inclusive podendo colocar em risco vidas humanas.

Desta forma, torna-se clara a necessidade da proposição de novas técnicas, metodologias e/ou soluções que visem tratar os desafios de segurança impostos pela Internet das Coisas de forma adequada as características deste paradigma.

A identificação, categorização e classificação de ameaças de segurança através de uma abordagem sistemática permite a antecipação, ainda em fase de *design*, aos cenários de ameaças aos quais um sistema está potencialmente exposto. Além disto, permite também a avaliação do estado atual do sistema frente as possíveis ameaças de segurança. Adicionalmente, a utilização de uma metodologia de modelagem de ameaças de segurança permite a priorização dos esforços de segurança, a justificativa para as tomadas de decisões estratégicas de segurança e a maior assertividade na implantação de recursos de segurança, uma vez que as ameaças identificadas partem de uma visão diretamente ligada à arquitetura do sistema, sob a ótica de um potencial atacante.

Partindo da primitiva de que a utilização de que uma metodologia de modelagem de ameaças adaptada à Internet das Coisas poderá migrar os benefícios desta técnica para o auxiliar na tratativa de questões de segurança, identificou-se uma lacuna no que se refere à utilização desta técnica no contexto da Internet das Coisas.

As metodologias de propostas generalistas, ou seja, propostas para contextos que não Internet das Coisas, possuem características que dificultam a utilização destas para a realização de modelagem de ameaças de segurança em ambientes IoT. Por exemplo, metodologias como a da Microsoft consideram categorias de ataques mais comuns ao desenvolvimento de *software* e um esquema de classificação de ameaças que se baseia nas principais ameaças voltadas a este contexto. Tais propriedades podem, por exemplo, não ser aplicáveis ou não ser suficientes para uma modelagem de ameaças adequada quando se trata de ambientes IoT. Tais metodologia são apresentadas no capítulo 3, o qual discorre sobre os trabalhos relacionados.

Embora alguns trabalhos como (CHOWDHURY; MACKENZIE, 2014; WANG; ALI; KELLY, 2015; SÁNDOR; SEBESTYÉN-PÁL, 2017) utilizem modelagem de ameaças para tratar de aspectos de segurança abordados em suas pesquisas, as metodologias utilizadas por estes pesquisadores limitam-se a um contexto específico no universo de IoT. Isto, por sua vez, impossibilita a generalização das metodologias utilizadas por estes pesquisadores e a sua consequente reutilização em outros contextos.

Com isto, a não identificação de uma metodologia de modelagem de ameaças de segurança, que possibilite a utilização desta abordagem mais amplamente em ambientes IoT, serviu de motivação principal para o desenvolvimento deste trabalho. Assim, este trabalho define como problema de pesquisa a seguinte questão: como realizar a modelagem de ameaças de segurança em ambientes baseados na Internet das Coisas através de uma metodologia geral, considerando as propriedades inerentes a este novo paradigma da computação?

1.3 Objetivos

Nesta seção são apresentados o objetivo geral e os objetivos específicos que serão utilizados para guiar o desenvolvimento deste trabalho.

1.3.1 Objetivo Geral

- Elaborar uma metodologia de modelagem de ameaças de segurança mais amplamente aplicável em ambientes baseado na Internet das Coisas.

1.3.2 Objetivos Específicos

- Analisar as metodologias de modelagem de ameaças existentes, tanto em contextos gerais quanto no âmbito da Internet das Coisas;
- Analisar a adequação dessas metodologias ao contexto de modelagem de ameaças de segurança em ambientes IoT;
- Avaliar a metodologia proposta através de um estudo de caso.

1.4 Estruturação do Trabalho

O capítulo 2 discorre sobre os conceitos básicos necessários para compreender o contexto da pesquisa. Neste capítulo, serão apresentados conceitos sobre segurança da informação, Internet das Coisas, modelagem de ameaças e outros conceitos que ajudam o entendimento do trabalho proposto.

O capítulo 3 apresenta os principais trabalhos relacionados, os quais foram utilizados como referência para o entendimento do estado da arte, construir a contextualização do trabalho e identificar da problemática que procura ser tratada neste trabalho de pesquisa. Neste capítulo, também é exposta a análise comparativa destes trabalhos em termos de suas propostas e de sua adequação à Internet das Coisas.

A metodologia proposta neste trabalho será apresenta no capítulo 4. Esta seção apresentará o processo utilizado para o uso desta metodologia e a visão geral de sua estrutura. O capítulo também discorrerá sobre a especificação de cada atividade definida como parte do processo de modelagem proposto.

No capítulo 5, será especificado o estudo de caso utilizado para avaliar a metodologia proposta. O estudo de caso tem a função tanto de ilustrar a metodologia proposta como avaliar a mesma.

Por fim, o capítulo 6 discorrerá sobre as conclusões deste trabalho e possibilidades de encaminhamentos futuros.

2 Conceitos Básicos

Neste capítulo serão apresentados os principais conceitos necessários para o entendimento deste trabalho. Dentre a fundamental conceitual, serão apresentados conceitos sobre Internet das Coisas, segurança da informação, modelagem de ameaças e noções de da notação BPMN.

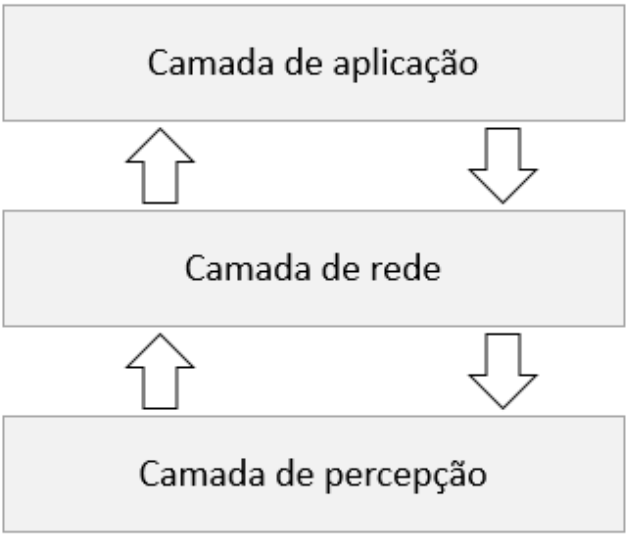
2.1 Internet das Coisas

A Internet das Coisas pode ser entendida como a interconexão de dispositivos físicos, que coletam e trocam dados entre si através de sua conectividade à Internet (SAIN; KANG; LEE, 2017) . Em outras palavras, a Internet das Coisas pode também ser vista como a interconexão de dispositivos, pessoas e serviços, que podem interagir entre si a qualquer hora, em qualquer lugar, com qualquer coisa (ABOMHARA; KØIEN, 2014).

Embora a pilha de protocolo TCP/IP tenha servido de base para o que foi alcançado em termos de serviços e aplicações até os dias atuais, a proposta de heterogeneidade e ubiquidade proposta pela Internet das Coisas requer novos padrões de arquiteturas e protocolos. Garantia de qualidade de serviço, suporte a mecanismos de endereçamento único e global das coisas, inclusão de requisitos de segurança como privacidade e integridade, são alguns dos exemplos dos diversos requisitos exigidos para adoção desde paradigma.

Embora existam diversas propostas de arquiteturas, grande parte dos autores concordam com a definição básica da arquitetura de três camadas, a qual representa a visão arquitetural da Internet das coisas (IRSHAD, 2016; KRAIJAK; TUWANUT, 2015). Tal visão arquitetural pode ser descrita pela camada de percepção, camada de rede e camada de aplicação.

Figura 1 – Representação da arquitetura de três camadas da Internet das Coisas



Fonte: Produzido pelo autor.

A camada de percepção representa a camada de mais baixo nível da arquitetura. O objetivo principal desta camada é coletar os dados que serão enviados, processados e utilizados pelas diversas aplicações suportadas pela Internet das Coisas. Dentre as principais tecnologias que permitem a coleta de dados, temos a presença de sensores, transmissores, *tags* RFID e NFC, GPS, sensores infravermelho, dentre outras.

Já a camada de rede representa o centro da arquitetura da Internet das Coisas e é responsável pela transmissão de forma rápida, segura e confiável dos dados trafegados entre as camadas de percepção e de aplicação. Para isto, deve-se garantir a interoperabilidade entre as diversas tecnologias de rede e telecomunicação. Em seu trabalho, Kraijak e Tuwanut (2015) pontuam que a camada de rede deve ser capaz de suportar dois principais tipos de transmissão de dados: transmissão de dados a curta distância e transmissão de dados remota. Segundo os autores, a transmissão de dados à curta distância depende principalmente de tecnologias de rede sem fio, como Wi-fi, Bluetooth, Ad-hoc, Mesh e Zigbee. Já a transmissão de dados remota é constituída por tecnologias que suportem, por exemplo, a transmissão de dados móveis e redes de comunicação via satélite.

A camada de aplicação representa a camada de mais alto nível da arquitetura da Internet das Coisas. É papel desta camada processar os dados colhidos pela camada de percepção e recebidos através da camada de rede e fornecer estes dados de forma utilizável pelos serviços que tangem diversos domínios de aplicação da Internet das Coisas. Dentre os principais domínios de aplicação, destacam-se as aplicações em *healthcare*, transporte, ambientes inteligentes (casas e cidades inteligentes) e nos

domínios sociais e pessoais (ATZORI; IERA; MORABITO, 2010).

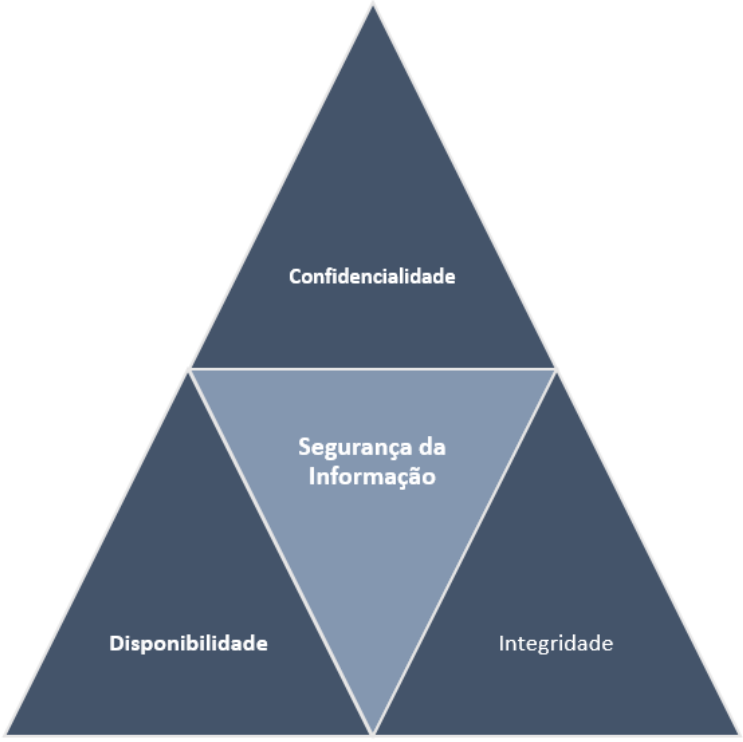
2.2 Segurança da Informação

Segurança da informação se refere a toda e qualquer proteção existente sobre as informações. Com isto, entende-se por informação todo conteúdo que tenha um dado valor para o seu proprietário (REIS, 2011).

Em uma visão mais geral, a segurança da informação é constituída por três princípios fundamentais: confidencialidade, integridade e disponibilidade. Tais princípios são definidos a seguir:

- Confidencialidade: propriedade que visa garantir que a informação não seja acessível a indivíduos, entidades ou processos não autorizados. A confidencialidade deve ser preservada para cada unidade de dados e deve ser mantida enquanto os dados estão armazenados em um sistema, quando são transmitidos e quando chegam ao seu destinatário.
- Integridade: integridade se refere a consistência do estado da informação. Toda e qualquer modificação não autorizada dos dados, seja ela intencional ou não, é considerada uma violação deste princípio.
- Disponibilidade : visa garantir que a informação esteja disponível quando necessário.

Figura 2 – Representação dos princípios da segurança da informação



Fonte: Produzido pelo autor.

2.3 Modelagem de ameaças

Método que consiste na identificação, categorização e classificação de ameaças de segurança relacionadas a um objeto de análise e, baseado neste conhecimento, a determinação das técnicas, métodos e algoritmos de mitigação de ameaças de segurança (SÁNDOR; SEBESTYÉN-PÁL, 2017).

2.3.1 Ativo

Um ativo é compreendido por um recurso que possua valor para o seu dono. Geralmente, um ativo pode ser entendido através de três diferentes visões: sinônimo para um dispositivo computacional, um recurso considerado de valor no sistema e que deseja proteger, ou um alvo de interesse de um atacante.

A partir dessas diferentes visões, um ativo pode ser visto, por exemplo, como uma informação, a disponibilidade desta informação, ou o dispositivo que armazena esta informação.

2.3.2 Vulnerabilidade

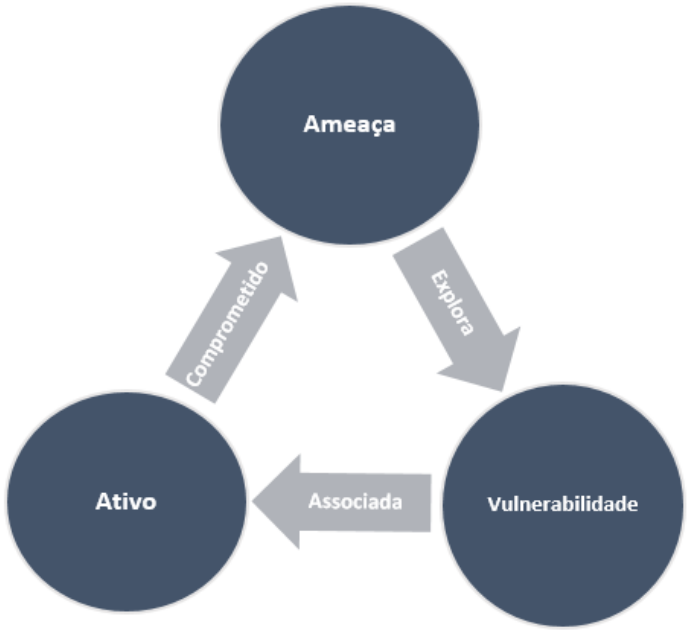
Vulnerabilidade representa uma falha de segurança presente em um determinado ativos, a qual pode ser explorada por um atacante, seja intencionalmente ou não, resultando assim na quebra de um ou mais dos princípios da segurança da informação. Por exemplo, a não utilização de protocolos de criptografia durante a comunicação entre *hosts* é uma vulnerabilidade que pode permitir, por exemplo, que um possível atacante obtenha dados sensíveis sobre as partes envolvidas, como credenciais de acesso.

2.3.3 Ameaça

Ameaça é o termo utilizado para representar situações que podem pôr em risco a tríade de Confidencialidade, Integridade e Disponibilidade da informação. Uma ameaça explora uma vulnerabilidade associada a um ativo do sistema.

A imagem a seguir retrata o relacionamento entre os conceitos de ativo, ameaça e vulnerabilidade. De forma geral, uma ameaça de segurança explora uma vulnerabilidade que está diretamente associada a um ativo do sistema.

Figura 3 – Relação entre ativo, ameaça e vulnerabilidade



Fonte: Produzido pelo autor.

2.3.4 Ataque

Um ataque se caracteriza por uma ação tomada por algo ou alguém e que visa danificar um ativo utilizando uma ou mais vulnerabilidades para concretizar um cenário de ameaça. Por exemplo, um atacante pode utilizar ferramentas de geração de tráfego automático com o intuito de realizar um ataque de negação de serviço contra um sistema IoT.

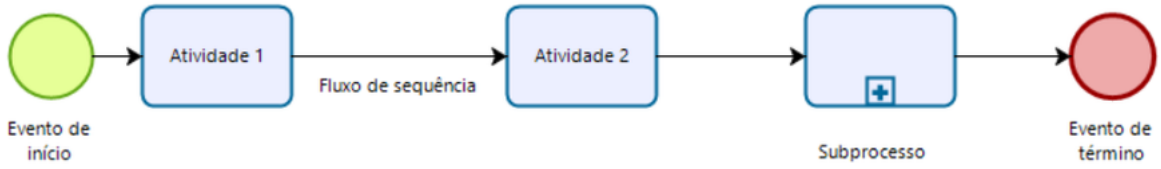
2.3.5 Contramedida

Medida de segurança adotada para mitigar uma vulnerabilidade e, consequentemente, diminuir ou extinguir as possibilidades de exploração de um ativo por uma determinada ameaça de segurança associada.Por exemplo, com o intuito de mitigar ameaças à privacidade e confidencialidade, pode-se utilizar protocolos de criptografia durante a comunicação entre as entidades do sistema.

2.4 Noções de BPMN

BPMN, ou *Business Process Model and Notation,* é uma notação padrão desenvolvida pela Object Management Group para a modelagem de processos de negócio (OBJECT MANAGEMENT GROUP, 2011). Para a representação da metodologia proposta por este trabalho, foram utilizados elementos da notação BPMN para representar o fluxo das atividades definidas. Os principais elementos da notação BPMN utilizados neste trabalho estão representados na Figura 4:

Figura 4 – Exemplo da utilização de elementos da notação BPMN



Fonte: Produzido pelo autor.

Onde:

- Evento - Eventos descrevem um acontecimento no fluxo de um processo. Existem três eventos principais na notação BPMN, são eles: eventos de início, eventos intermediários e eventos de término. Eventos de início representam o início de um processo. Processos intermediários definem eventos que ocorrem durante o fluxo do processo. Já eventos de término representam o fim do fluxo de um

processo. Para o contexto deste trabalho, apenas foram utilizados os eventos de início e término de processo;

- Atividade - Uma atividade representa uma ação realizada no fluxo de um processo. Por exemplo, a atividade representada pela Atividade 1 poderia indicar a ação “Enviar e-mail”;
- Fluxo de sequência - Indica a ordem em que as atividades devem ser execução em um processo;
- Subprocesso - Um subprocesso é uma atividade composta por um conjunto de subatividades que podem ser representadas por um fluxo de processo próprio.

3 Trabalhos Relacionados

Neste capítulo, serão apresentados os principais trabalhos relacionados, os quais foram utilizados para a compreensão do estado da arte desta área de pesquisa, para construção e fundamentação teórica e para identificação da problemática que procura ser solucionada neste projeto de pesquisa.

Para um melhor entendimento, este capítulo foi dividido em três seções: a seção 3.1 discorre sobre o contexto geral de modelagem de ameaças, apresentando as principais metodologias propostas para contextos outros que não IoT. Já a seção 3.2 apresenta o contexto atual de modelagem de ameaças no cenário de IoT. Por fim, a seção 3.3 apresenta técnicas auxiliares envolvidas no processo de modelagem de ameaças.

3.1 Propostas generalistas para modelagem de ameaças

A Microsoft propõe um guia detalhado para a realização de modelagem de ameaças para softwares, como parte do SDL (*Security Development Lifecycle*) de aplicações. Em sua abordagem, a Microsoft define o processo geral de modelagem de ameaças de aplicações em 6 passos: Identificar ativos, criar uma arquitetura geral da aplicação, decompor a aplicação, identificar as ameaças, documentar as ameaças e classificar as ameaças. A saída deste processo consiste em um modelo de ameaça composto pela visão arquitetural do sistema e uma lista de ameaças associadas à aplicação de forma categorizada e classificada por severidade. Um modelo de ameaças de uma aplicação permite a clara compreensão das ameaças que necessitam ser tratadas, em qual prioridade precisam ser tratadas e como mitigá-las(MICROSOFT, 2003).

A primeira etapa desta metodologia visa identificar os ativos do sistema que se deseja proteger. Estes ativos podem ser, por exemplo, páginas Web, o servidor de banco de dados da aplicação, etc. A partir da identificação dos ativos, a metodologia da Microsoft propõe a criação de uma arquitetura geral da aplicação. Esta fase tem por objetivo identificar para que a aplicação é proposta e como ela usa e acessa os ativos identificados na primeira etapa do processo. Como saída desta fase, espera-se um diagrama de alto nível da composição e estrutura da aplicação, seus subsistemas, juntamente com as principais tecnologias utilizadas pela aplicação.

A fase de decomposição busca uma visão mais aprofundada do sistema e a criação de um perfil de segurança. Assim, essa etapa se destina a identificação do fluxo de dados, pontos de entrada, fronteiras de confiança (tradução livre de *trust boundaries*)

e códigos privilegiados da aplicação. A partir do insumo dessas informações, deve-se então criar um perfil de segurança do sistema. O perfil de segurança visa documentar considerações de design da aplicação no que se refere a validação de entradas do usuário, mecanismos de autenticação e autorização, gerenciamento de configuração, gerenciamento de sessão, mecanismos de criptografia, manipulação de parâmetros, gerenciamento de exceções e mecanismos de auditoria e *logging* da aplicação.

Em seguida, para a fase de identificação de ameaças, a Microsoft recomenda a utilização do esquema de categorização de ameaças STRIDE. O acrônimo STRIDE é formado pelas iniciais das seguintes categorias de ameaças: *spoofing, tampering, repudiation, information disclosure, denial of service* e *elevation of privilege.*

Posteriormente, na fase de documentação das ameaças, a companhia fornece um *template* destinado ao registro das ameaças identificadas. O formato apresentado para a documentação das ameaças registra a descrição da ameaça, o alvo da ameaça, o risco associado à ameaça, o ataque utilizado para gerar o cenário de ameaça e contramedida à ameaça em questão.

Por último, encontra-se a etapa de classificação de ameaças. Nesta fase do processo, com os insumos providos pela identificação das ameaças realizada no passo anterior, deve-se então classificar as ameaças por criticidade. Para isso, a Microsoft recomenda a utilização do método de classificação DREAD. O acrônimo DREAD refere-se as seguintes propriedades que devem ser consideradas para classificar uma ameaça: *damage potential, reproducibility, exploitability, affected users* e *discoverability*.

Cada propriedade citada deve receber um valor equivalente a ‘0’, ‘5’ ou ‘10’. Por fim, para calcular o risco, deve-se somar os valores atribuídos a cada uma das propriedades e dividir o valor da soma por ‘5’. Adicionalmente, a Microsoft cita esquemas de classificação alternativos como através da fórmula *Risk = probability * damage potential* ou a atribuição dos valores de *High, Medium* ou *Low* para cada ameaça em particular. Realizando este processo para cada uma das ameaças, resulta-se então em uma lista de ameaças classificadas pelo seu grau de severidade.

Embora a metodologia proposta pela Microsoft seja um guia interessante para modelagem de ameaças, esta não se adequa totalmente ao contexto de IoT. Uma vez que essa metodologia foi proposta para o contexto do desenvolvimento seguro de *software* (mais especificamente, aplicações Web), ela foi projetada para tratar das ameaças inseridas neste universo. Isto implica dizer que a compreensão, identificação, categorização e classificação das ameaças podem diferir do contexto a que essa metodologia foi proposta para o contexto de IoT. Por exemplo, o modelo de categorização utilizado na fase de identificação de ameaças chamado STRIDE pode não incluir categorias de ameaças presentes no universo de IoT. Adicionalmente, o método de classificação DREAD, utilizado para classificar as ameaças por severidade, pode não

incluir fatores que agreguem ou não a severidade de uma determinada ameaça no contexto de IoT (SÁNDOR; SEBESTYÉN-PÁL, 2017).

A OWASP (2003) também possui uma definição do processo de modelagem de ameaças estabelecido e disponível em seu acervo online, o qual é baseado na metodologia proposta pela Microsoft. Assim, a OWASP pontua que o *Threat Risk Modeling* é um processo essencial para prover segurança no desenvolvimento de uma aplicação Web, permitindo que as organizações priorizem seus esforços de segurança de acordo com o orçamento disponível. De acordo com o proposto pela organização, o processo de modelagem de ameaças é composto por cinco passos: identificação dos objetivos de segurança, criação de um *overview* da aplicação, decomposição da aplicação, identificação de ameaças e identificação de vulnerabilidades(OWASP, 2006).

Por fim, segundo a OWASP, deve-se identificar contramedidas e estratégias de mitigação das ameaças. O propósito da identificação de contramedidas é determinar as possíveis medidas de proteção que podem ser adotadas para prevenir a ocorrência de cada ameaça identificada nas fases anteriores. Para isto, pode-se utilizar a lista de contramedidas proposta pelo STRIDE ou a lista disponível pelo *Application Security Frame* (ASF) da Microsoft. Por último, deve-se determinar qual estratégia de mitigação será escolhida para cada ameaça. As possíveis escolhas são: ignorar o risco, informar a respeito do risco, mitigar o risco, aceitar o risco, transferir o risco ou finalizar o risco.

Assim como a metodologia de modelagem de ameaças proposta pela Microsoft, a metodologia apresentada pela OWASP enfrenta questões similares no que concerne a sua adaptação ao contexto de IoT pelas mesmas razões citadas anteriormente. Com isto, embora a organização forneça um guia detalhado para modelagem de ameaças que servirá de base para a criação de uma nova metodologia, a compreensão, identificação, categorização e classificação das ameaças diferem do contexto a que essa metodologia foi proposta para o contexto de IoT.

Ao contrário das metodologias de modelagem de ameaças citadas anteriormente, o framework Trike, proposto por Saitta, Larcom e Eddington (2005), utiliza de uma abordagem focada no gerenciamento de riscos para propor uma abordagem para modelagem de ameaças. Trike é um *framework* conceitual que parte da visão de gerenciamento de riscos, destinado a auxiliar na realização de auditorias de segurança. Este framework busca a automação de partes do processo de modelagem de ameaças, possibilitado pelo alto grau de formalidade buscado nas etapas do processo proposto e pelo suporte provido através da ferramenta desenvolvida para dar apoio a este processo de modelagem.

O processo proposto pelo Trike é constituído das seguintes etapas: Modelo de requisitos, Modelo de implementação, Modelo de ameaças e Modelo de riscos. Na etapa de elaboração do modelo de requisitos, o Trike visa especificar os atores, ativos,

as ações pretendidas dos atores e as regras que definem em que circunstância uma ação pode ocorrer. Essas informações são posteriormente organizadas em uma matriz (chamada de ator-ativo-ação), onde as colunas da matriz representam os ativos do sistema e as linhas representam os papéis que atores podem se enquadrar. Com isto, esta etapa visa prover o entendimento do que o sistema é proposto a realizar, quem interage com o sistema, quais ações realizadas por estes atores o sistema é proposto a suportar e quais regras estão implementadas para suportar tais ações.

Após a formalização do modelo de requisitos, o Trike propõe a construção do modelo de implementação. Esta etapa visa entender como o sistema está implementado. A primeira etapa da construção do modelo de implementação é identificar as ações suportadas pelo sistema e a forma como essas ações alteram o seu estado e, com isto, construir uma máquina de estados do sistema analisado. Depois da construção da máquina de estados do sistema, deve-se então construir o diagrama de fluxo de dados (do inglês *Data Flow Diagrams*). A utilização de DFDs visa prover uma visão lógica e de alto nível da arquitetura do sistema, especificando como as entidades do sistema estão dispostas e como ocorre o fluxo de informações entre essas entidades.

Depois, o modelo de implementação é analisado para produzir o modelo de ameaças. No Trike, o conjunto de ameaças associadas a um sistema é puramente determinístico, dada a matriz de ator-ativo-ação. Existem apenas duas categorias de ameaças onde as ameaças são mapeadas neste *framework*, sendo elas negação de serviço e elevação de privilégio. Posteriormente, cada ameaça identificada se torna um nó raiz em uma árvore de ataque, que por sua vez é composta por descrições hierárquicas de ataques que um possível atacante deve realizar para conseguir gerar o cenário de ameaça. As árvores de ameaça por sua vez são utilizadas para compor o grafo de ameaças do sistema. Por fim, as fraquezas, vulnerabilidades e mitigações são identificadas.

Por último, dados os insumos das etapas anteriores, o modelo de riscos é produzido. Esta fase busca determinar o nível de exposição de cada ameaça e as probabilidades que estão associadas com as vulnerabilidades que a implementam. Dado este entendimento, o valor do risco de ameaça pode ser calculado a partir da multiplicação entre o nível de exposição de uma ameaça e a maior probabilidade dentre as vulnerabilidades que compõem esta ameaça, concluindo o processo proposto pelo Trike.

O framework Trike apresenta uma visão defensiva do sistema, sob uma perspectiva de gerenciamento de riscos. Com o intuito de auxiliar no processo de auditoria de segurança, o formalismo apresentado pelo Trike é um ponto forte desta metodologia. A formalização do sistema em máquinas de estados e, posteriormente, diagrama de fluxo de dados auxiliam na compreensão exata de como o sistema é proposto a ser utilizado.

A proposta de automação das etapas de geração de ameaças e dos grafos de ameaças do sistema, caso funcionem como o especificado, pode permitir que analistas/auditores percam menos tempo nessas etapas do processo, permitindo a priorização do tempo na análise, classificação e consequente mitigação das ameaças associadas ao sistema.

Contudo, a metodologia apresentada pelo Trike está em fase experimental, onde os autores afirmam que partes do processo ainda não foram testadas em ambientes reais, o que prejudica a assertividade da proposta do Trike. A proposta de automação das etapas de geração de ameaças e de grafos de ameaças pode ser comprometida, uma vez que dependem do alto grau de formalismo e especificação das etapas de geração do modelo de requisitos e de implementação do sistema. Adicionalmente, há uma aparente falta de documentação e suporte a esta metodologia, uma vez que existem menções à versão do Trike 2.0, mas só existe o *draft* da versão 1.0 disponibilizada pelos autores.

Observa-se também que, dado o grau de formalismo proposto pelo Trike, principalmente no que se concerne a produção de uma máquina de estados de um sistema, pode levar ao aumento da complexidade da aplicação desta abordagem em ambientes que possuem maior número de entidades envolvidas, como é o caso de IoT. Por fim, a ferramenta de suporte ao Trike, chamada *Squeak*, não possui documentação de referência que auxilie o processo de testes e possível modelagem através desta ferramenta.

A Tabela 1 compara as metodologias apresentadas durante esta seção em termos das principais características adotadas por cada uma:

Tabela 1 – Tabela de comparação entre atributos das metodologias de modelagem de ameaças de contexto geral

Metodologia	**Método de representação da arquitetura**	**Método de identificação de ameaças**	**Método de categorização de ameaças**	**Método de classificação de ameaças**
Microsoft (2003)	DFD	STRIDE	STRIDE	DREAD
OWASP (2006)	DFD	STRIDE	STRIDE	DREAD
Trike(2005)	Máquina de estados e DFD	Automática através da ferramenta proprietária Squeak	Negação de serviço e Elevação de privilégios	Nível de exposição x maior probabilidade dentre as vulnerabilidades que compõe a ameaça

Fonte: Produzido pelo autor.

3.2 Cenário de modelagem de ameaças no contexto de IoT

No cenário de IoT, poucos trabalhos se voltam à realização de modelagem de ameaças. O trabalho proposto por Wang, Ali e Kelly (2015) investiga questões de segurança da informação no contexto de cidades inteligentes a partir de uma perspectiva técnica e de operação organizacional. Dada a compreensão destes problemas, os autores propõem uma abordagem para analisar ameaças de segurança a que esses ambientes estão expostos, visando a otimizar a segurança dos dados em cidades inteligentes. Ao término do estudo, os autores apresentam resultados de experimentos realizados e afirmam que a aplicação da abordagem proposta pode auxiliar na significativa redução do fator de ameaça.

Neste trabalho, os autores propõem uma nova abordagem para avaliação e mitigação de riscos chamada HiSPO (*Hardware*, *intelligence*, *Software*, *Policies*, *Operation*). Esta abordagem utiliza um algoritmo desenvolvido pelos autores para calcular de forma automática o que é definido pelos autores como fator de ameaça de uma infraestrutura de cidade inteligente. O algoritmo utiliza dados recolhidos de redes, sistemas operacionais, esquemas de bancos de dados, políticas de segurança, operações de negócio, dados corporativos e de arquitetura de sistemas.

Após o processo de coleta de dados, um processo de modelagem de ameaças é iniciado. Para o processo de modelagem de ameaças realizado neste trabalho, são utilizadas informações sobre a topologia da rede, arquitetura do sistema, sistemas operacionais e atualizações, configurações e componentes de aplicações, armazenamento de dados, mecanismos de criptografia, dentre outros.

Dada a modelagem de ameaças do ambiente, uma lista contendo os riscos e suas ameaças associadas é gerada. As ameaças são então divididas nas seguintes categorias: *spoofing, DoS,* elevação de privilégios e *tampering*. Em seguida, as ameaças são categorizadas em "*high risk*", *"medium risk",* ou *"low risk".*

De acordo com os autores, no primeiro mês de um experimento realizado, as avaliações e mitigações conduzidas utilizando a abordagem proposta levaram a redução do fator de ameaça de 0.71 para 0.38. Contudo, após esta primeira rodada, a equipe de avaliação ainda era capaz de extrair dados sensíveis do sistema. Com isto, uma segunda rodada de avaliação e mitigação foi realizada em três meses, reduzindo o fator de ameaça para 0.18. Neste ponto, segundo o relato, a equipe de testes não conseguiu mais extrair dados do sistema, indicando a dificuldade associada a um possível vazamento de dados para o contexto de cidade inteligente onde o estudo foi realizado.

Em um outro trabalho, realizado por Chowdhury e Mackenzie (2014), os autores desenvolvem um modelo de ameaças voltado à Accident Warning Systems (AWSs)

baseado em redes Ad-hoc. Sistemas AWSs utilizam redes veiculares Ad-hoc para auxiliar na prevenção de potenciais colisões de trânsito e na propagação de notificações e alertas de segurança entre veículos. Inicialmente, é realizada uma pesquisa acerca de AWSs, buscando compreender os principais conceitos que envolvem esses sistemas e entender sua arquitetura básica. Posteriormente, os autores buscam identificar os principais tipos de atacantes e os possíveis ataques que possam utilizar contra esse tipo de sistema. Por fim, o trabalho propõe um modelo de ameaças que objetiva apresentar uma visão de como a segurança, privacidade e confiança em AWSs podem ser afetadas e de como esses pilares podem ser protegidos.

Dada as características dos sistemas AWSs, seus potenciais atacantes foram categorizados de acordo com os danos que poderiam causar a esses tipos de sistemas. As categorias definidas pelos autores foram: Ameaças de primeiro grau, ameaças de segundo grau e ameaças de terceiro grau.

A partir dos insumos sobre potenciais atacantes e os tipos de ataques que sistemas AWSs estão expostos, os autores apresentam um modelo de ameaças genérico para AWSs. O modelo de ameaças produzido visa oferecer um entendimento mais claro sobre o relacionamento entre as categorias de atacante, os possíveis ataques que possam realizar e quais aspectos dentre privacidade, segurança e confiança podem ser comprometidos através destes ataques.

Em um trabalho mais recente, realizado por Sándor e Sebestyén-Pál (2017), é realizada uma adaptação do processo de modelagem de ameaças proposto pela Microsoft para o contexto do IoT. Esta adaptação do processo de modelagem de ameaças é parte de proposta principal dos autores, que visam definir um algoritmo para determinar a configuração de segurança mais adequada de um sistema levando em consideração perfis de segurança e o custo de sua adoção. Os autores partem da premissa de que a adoção e adaptação de técnicas tradicionais de segurança, como a modelagem de ameaças, podem contribuir fortemente para a proposição de soluções de segurança em IoT.

Baseados na metodologia de modelagem de ameaças apresentada pela Microsoft, os autores realizam a adequação de algumas de suas etapas como forma de adaptá-la à Internet das Coisas. As principais alterações entre a metodologia da Microsoft e a metodologia proposta no trabalho destes pesquisadores foram ajustes no esquema de classificação DREAD.

O esquema de classificação usado pelo DREAD utiliza-se de três categorias e seus respectivos pesos para atribuir valores às ameaças analisadas: *Low = 1, Medium =2* e *High =3.* Os pesquisadores realizam a adequação deste esquema de classificação, estendendo o esquema base, adicionando ou ajustando os critérios de valoração das ameaças, como descrito na Tabela 2. Os campos que apresentam o caractere '*'

representam adições ou extensões realizadas pelos autores. Após o ajuste, os autores propõem o seguinte esquema de classificação:

Tabela 2 – Questionário DREAD modificado para IoT

Classes	*Ignore (0)	Low(1)	Medium(2)	High(3)
Da	* Atividade sem nenhum dano	* Vazamento trivial de informações acerca do ativo IoT e/ou usuários	* Vazamento de informação sensível acerca de coisas e/ou usuários, ou perda de qualquer tipo de informação	* Permite que um atacante comande um dispositivo IoT e obtenha total autorização, execute com privilégios administrativos
R	*Para o componente afetado, existe mecanismos de proteção disponíveis contra o ataque	O ataque é difícil ou impossível de reproduzir	O ataque apenas pode ser reproduzido com uma janela de tempo específica e uma condição de corrida particular	O ataque pode ser reproduzido a qualquer momento
E	* Mesmo que haja probabilidades estatísticas de exploração, o ataque requer diversos recursos que por sua vez são probabilisticamente menos disponíveis	O ataque requer uma pessoa com profundo conhecimento técnico ou com conhecimento interno do sistema todas as vezes para realizar a exploração	Uma pessoa tecnicamente hábil, como um programador, pode realizar o ataque e, posteriormente, repetir os passos de exploração	Um programador iniciante ou pessoas sem conhecimento técnico podem realizar o ataque em tempo hábil seguindo um guia

Classes	*Ignore (0)	Low(1)	Medium(2)	High(3)
*A	* O ataque não afeta nenhum usuário ou coisas	* Um pequeno número de usuários ou coisas são afetados	* Um grupo, por exemplo, *subdomínio, de usuários ou coisas são afetados*	* Todos os usuários e / ou coisas *são afetadas*
Di	* Uma solução alternativa é aplicada que esconde/corrige o *bug/vulnerabilidade*	A vulnerabilidade tem comportamento difícil de ser entendido. Portanto, é muito difícil *compreender os possíveis danos potenciais de sua exploração*	A vulnerabilidade pode ser acessada por apenas alguns *usuários, e seria necessário esforço para enxergar o uso malicioso*	Guias publicados são *disponíveis para ataque, ou a vulnerabilidade é visível ou facilmente perceptível através da interface do usuário*

Fonte: Extraído de Sándor e Sebestyén-Pál (2017)

Os trabalhos realizados por Wang, Ali e Kelly (2015), o trabalho proposto por Chowdhury e Mackenzie (2014) e por Sándor e Sebestyén-Pál (2017), apresentam exemplos de aplicação de modelagem de ameaças no contexto da Internet das Coisas e ressaltam a importância da utilização desta técnica como uma solução para problemáticas de segurança em IoT. As metodologias adotadas pelos autores podem servir de insumo e base para a proposição de uma metodologia mais completa e aplicável aos demais contextos que requerem uma proposta de modelagem de ameaças no contexto da Internet das Coisas. Porém, as metodologias de modelagem de ameaças utilizadas nestes trabalhos são aplicáveis ao contexto a que são propostas, não servindo como uma metodologia mais abrangente para ambientes IoT. Com isto, este trabalho visa desenvolver e propor uma metodologia de modelagem de ameaças que não seja apenas aplicável a um contexto específico em IoT, sendo uma metodologia geral que possa ser aplicável e instanciada aos demais contextos da Internet das Coisas.

3.3 Técnicas auxiliares ao processo de modelagem de ameaças

O STRIDE é um método de categorização de ameaças proposto pela Microsoft. O principal intuito deste método é identificar e categorizar as ameaças a partir da visão dos objetivos de um potencial atacante. Este método é amplamente utilizado em

metodologias de modelagem de ameaças voltados a aplicações Web.

O acrônimo STRIDE é formado pelas iniciais das categorias de ameaças descritas a seguir:

- ***Spoofing -*** Ameaças que visem ganhar o acesso ao sistema usando identidades falsas. Por exemplo, um atacante que tem acesso ao sistema através de credenciais roubadas ou que se utiliza de um endereço IP falso.
- ***Tampering -*** Refere-se à adulteração de dados sem autorização. Por exemplo, um atacante que realiza um ataque man-in-the-middle e altera as informações que fluem entre o cliente e o servidor.
- ***Repudiation -*** É a habilidade de usuários (legítimos ou não legítimos) de negar que tenham executado alguma ação.
- ***Information Disclosure -*** Exposição não autorizada de dados.
- ***Denial of Service*:** Processos que visem tornar um sistema indisponível.
- ***Elevation of Privilege -*** Ocorre quando um usuário com privilégios limitados consegue executar ações com o nível de privilégios de um usuário com maiores permissões.

Cada uma das categorias de ameaças descritas pelo STRIDE possui um conjunto de contramedidas proposto para auxiliar na redução dos riscos. Cada contramedida apresentada depende do ataque específico identificado.

A empresa também disponibiliza um conjunto de categorias de ameaças e contramedidas específicas para as ameaças na rede, no host e na aplicação. O conjunto de ameaças da rede é composto pelas categorias: acúmulo de informações, *sniffing*, *spoofing*, sequestro de sessões e negação de serviço. Já o conjunto de ameaças no host é formado pelas categorias: vírus, cavalo de Tróia e *worms*, *footprinting*, elaboração de perfil, quebra de senha, negação de serviço, execução maliciosa de códigos arbitrários e acesso não autorizado. Desta forma, a Microsoft apresenta um método de identificação e categorização de ameaças associadas às aplicações Web, assim como, possíveis contramedidas a estas ameaças de segurança.

O método de categorização de ameaças proposto pelo STRIDE apresenta uma visão clara das categorias de ameaças que podem estar associadas a uma aplicação Web e apresenta possíveis contramedidas às ameaças de segurança relacionadas a cada uma destas categorias. Isto permite entender como as ameaças são identificadas e como as contramedidas de segurança podem ser propostas a um determinado contexto.

Contudo, quando observado pela ótica deste trabalho, as categorias de ameaças e contramedidas de segurança para essas categorias podem sofrer variações. Apesar da similaridade de alguns tipos de ataques, e consequentemente cenários de ameaças, entre o contexto de aplicações Web e IoT, a taxonomia de ataques entre estes dois universos podem variar. Para o contexto deste trabalho, este método de categorização servirá como base para a proposição de um método de identificação de ameaças no contexto de IoT, levando em consideração a taxonomia de ataques e de ameaças relacionados especificamente para IoT.

O DREAD é um esquema de classificação de ameaças também utilizado no processo de metodologias de modelagem de ameaças como os propostos pela Microsoft, OWASP e OpenStack. O acrônimo DREAD refere-se as seguintes propriedades que devem ser consideradas para classificar uma ameaça:

- ***Damage Potencial*** – Quão grande é o dano caso a vulnerabilidade seja explorada?
  - Alto (3) – O atacante pode obter controle total do sistema; executar tarefas com privilégios administrativos;
  - Médio (2) – Perda de informações sensíveis;
  - Baixo (1) - Perda de informações triviais.
- ***Reproducibility*** – O quão fácil é reproduzir este ataque?
  - Alto (3) - O ataque pode ser reproduzido sempre ;
  - Médio (2) – O ataque só pode ser reproduzido com uma janela de *timing* específica e com uma condição particular;
  - Baixa (1) – O ataque é extremamente difícil de ser reproduzido, mesmo com amplo conhecimento em segurança.
- ***Exploitability*** – O quão fácil é executar o ataque?
  - Alta (3) – Um programador novato pode realizar um ataque em pouco tempo;
  - Médio (2) – Um programador experiente pode realizar o ataque e depois reproduzir os passos;
  - Baixo (1) – O ataque requer uma pessoa extremamente capacitada para realizar o ataque.
- ***Affected Users*** – Quantos usuários serão afetados?

  - Alta (3) – Todos os usuários, configuração padrão e principais clientes são afetados;
  - Média (2) – Alguns usuários e configuração não padrão são afetados;
  - Baixa (1) – Pequena porcentagem dos usuários são afetados.

- ***Discoverability*** – Quão fácil é achar esta vulnerabilidade?

  - Alta (3) – A vulnerabilidade é facilmente notável e fontes públicas explicam os meios de ataque;
  - Média (2) – A vulnerabilidade está contida em uma funcionalidade pouco acessível do sistema e requer bastante análise para que seja encontrada;
  - Baixa (1) – O *bug* que viabiliza a vulnerabilidade é obscuro e é altamente improvável que os usuários descubram potencias danos.

Por fim, para calcular o risco, deve-se somar os valores atribuídos a cada uma das propriedades e dividir o valor da soma por ‘5’.

Realizando este processo para cada uma das ameaças, resulta-se então em uma lista de ameaças classificadas pelo seu grau de severidade, permitindo a classificação de todas as ameaças coletadas na fase de identificação de ameaças.

O método de classificação DREAD propõe uma forma de classificar as ameaças em aplicações Web, levando em consideração propriedades importantes para este contexto. Contudo, assim como o método de categorização STRIDE, as propriedades utilizadas pelo DREAD para calcular a severidade de uma ameaça podem diferir de propriedades que sejam mais relevantes quando propõem-se a calcular a severidade de ameaças de segurança em IoT. Assim, este método servirá como insumos para a classificação de ameaças em IoT, levando em consideração os requisitos e propriedades que desejam ser observados para a própria classificação de ameaças de segurança em ambientes IoT.

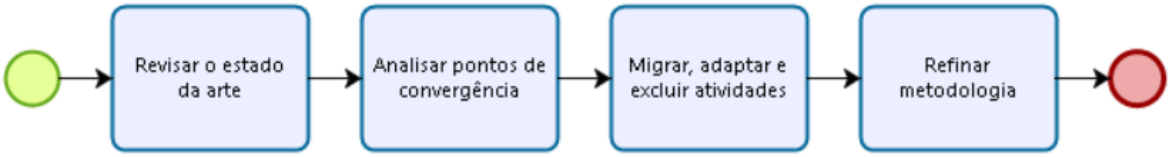
4 Metodologia para Modelagem de Ameaças de Segurança para Ambientes Baseados na Internet das Coisas

Este capítulo apresenta a proposta de metodologia em resposta ao problema de pesquisa definido neste trabalho. Primeiro, são apresentadas as atividades que foram necessárias para o desenvolvimento da metodologia. Posteriormente, é fornecida uma visão geral da metodologia proposta e também são apresentadas as definições de cada atividade envolvida nas etapas do processo de modelagem de ameaças de segurança aplicável a ambientes baseados na Internet das Coisas proposto neste trabalho.

4.1 Processo de desenvolvimento da metodologia

As principais atividades utilizadas para o desenvolvimento da metodologia proposta neste trabalho são apresentadas na Figura 5, são elas: revisão do estado da arte, análise dos pontos de convergência, migração, adaptação e exclusão de atividades e refinamento da metodologia.

Figura 5 – Processo de desenvolvimento da metodologia aplicável à Internet das Coisas



Fonte: Produzido pelo autor

4.1.1 Revisão do estado da arte

Em primeiro lugar, se fez necessário o entendimento do estado da arte no que se concerne as principais metodologias de modelagem de ameaças vigentes. A partir da observação da literatura, buscou-se a identificação dessas metodologias e o entendimento das atividades envolvidas no processo de modelagem proposto por estas.

Nesta atividade, foram consideradas tantos as metodologias em um cenário geral quanto as metodologias ou trabalhos que utilizam modelagem de ameaças no âmbito de IoT. Tais trabalhos, assim como suas respectivas descrições e análises, podem ser consultados no capítulo 3, o qual discorre sobre os trabalhos relacionados.

4.1.2 Análise dos pontos de convergência

Como estratégia para a proposição de uma metodologia aplicável a IoT, procurou-se identificar os pontos em que as metodologias analisadas convergiam. Em outras palavras, para a definição de uma metodologia base, foram mapeadas as atividades que estavam presentes em todas ou na maioria das metodologias analisadas. A partir desta estratégia, foi definida uma metodologia contendo as atividades base da metodologia inicial. Versão esta que foi posteriormente analisada em termos de sua adequação à IoT.

4.1.3 Migração, adaptação e exclusão de atividades

O objetivo principal desta atividade foi o de analisar as atividades que compunham a metodologia de modelagem de ameaça inicial em termos de sua adequação a IoT. Para isto, as atividades foram contrastadas com as propriedades inerentes ao paradigma da Internet das Coisas e foram alvos de três decisões estratégicas: exclusão da atividade, migração da atividade e adaptação da atividade.

Atividades excluídas, foram atividades que foram consideradas não aplicáveis ao contexto de IoT. A categoria de atividades migradas contemplou atividades em que não se observou a necessidade de adaptação para o contexto de IoT. Já as atividades passíveis de adaptação foram atividades que necessitaram de modificações para serem incluídas em uma metodologia voltada à IoT.

4.1.4 Refinamento da Metodologia

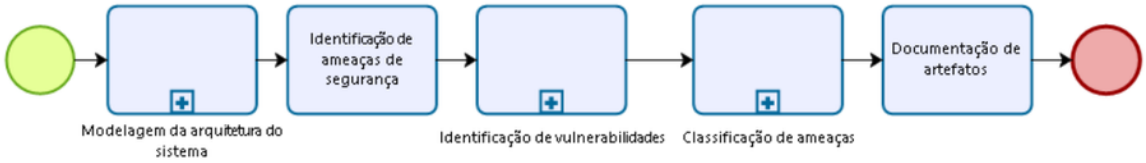
Após a migração da metodologia para o contexto de IoT, notou-se a necessidade de aprimoramentos em pontos da metodologia. A partir dos insumos providos da aplicação desta metodologia no estudo de caso proposto no capítulo, esta metodologia foi refinada para a sua melhor adequação ao contexto de IoT.

4.2 Visão Geral

A metodologia aplicável a IoT pode ser entendida a partir das seguintes subprocessos e atividades: Modelar arquitetura do ambiente IoT, identificar ameaças de segurança, identificar vulnerabilidades, classificar ameaças e documentar artefatos.

Para descrição, formalização e representação da metodologia proposta neste trabalho foi utilizada a notação BPMN. A Figura 6 demonstra a visão geral do processo que representa a metodologia:

Figura 6 – Visão geral da metodologia de modelagem de ameaças aplicável a Internet das Coisas



Fonte: Produzido pelo autor

Como saída do processo proposto nesta metodologia, espera-se um modelo de ameaças. O modelo de ameaças é um artefato composto pela visão arquitetural de alto nível do sistema e a lista de ameaças de segurança organizadas pelos seus respectivos riscos.

As seções a seguir serão destinadas ao detalhamento de cada um dos subprocessos e atividades especificados na Figura 5.

4.3 Modelagem da arquitetura do ambiente

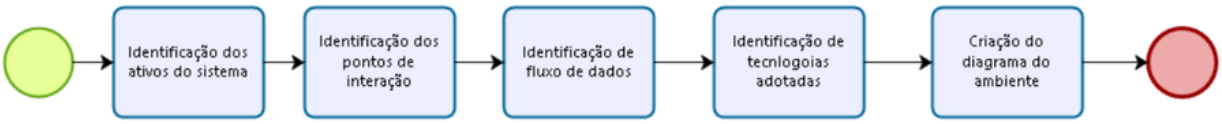
O primeiro subprocesso se destina a obter a compreensão do sistema sob análise. Para uma efetiva identificação de ameaças de segurança é necessário, primeiro, compreender quais são os componentes do sistema, como eles interagem, qual o fluxo de dados entre as principais entidades e quais os ativos que se deseja proteger. A partir desses insumos, é possível representar graficamente o sistema através de uma visão de alto nível.

Com isto, para a realização da etapa de modelagem da arquitetura do ambiente IoT, é recomendado consultar documentações que descrevam o ambiente tecnicamente. Dentre essas documentações, podem-se incluir: documentações de arquitetura do sistema, diagramas UML, diagramas de caso de uso, dentre outros.

Como saída principal deste subprocesso, espera-se a representação em alto nível da arquitetura do sistema analisado através da notação DFD.

Para isto, a metodologia proposta neste trabalho define as seguintes atividades a serem realizadas: Identificar componentes do sistema IoT, identificar pontos de interação com os componentes, identificar fluxo de dados, identificar tecnologias adotadas, criar diagrama do ambiente IoT e definir ativos. Figura 7 mostra a representação deste subprocesso:

Figura 7 – Atividades do subprocesso Modelar a arquitetura do ambiente IoT



Fonte: Produzido pelo autor

4.3.1 Identificação dos ativos do sistema

Ativos podem ser visto como recursos de valor para o seu dono e que podem ser alvo de potenciais atacantes. Para entender qual a composição do sistema baseado na Internet das Coisas, deve-se iniciar identificando quais são os ativos que formam a solução do sistema em questão.

Estes componentes podem ser dispositivos IoT (como sensores, atuadores, tags RFID), servidores, entidades na nuvem, *gateways,* banco de dados, etc. Desta forma, como principal saída desta atividade, espera-se uma lista destes componentes identificados. Os componentes identificados nesta atividade serão utilizados para mapear os pontos de interação e o fluxo de dados no sistema, os quais serão representados posteriormente através do diagrama arquitetural do sistema em análise.

Definir os ativos é uma das etapas mais importantes do processo de modelagem pois a identificação de ameaças de segurança será baseada na representação da arquitetura do sistema, a qual será constituída pelos ativos levantados nesta fase.

4.3.2 Identificação dos pontos de interação

Esta atividade visa identificar pontos de interação entre os usuários e os dispositivos IoT, entre os dispositivos e sistemas externos, entre os próprios ativos, ou entre os dispositivos do sistema e o ambiente. Por exemplo, uma página Web que permita interagir remotamente com o dispositivo IoT, uma porta de rede que associada a algum serviço em execução, ou um sensor de temperatura utilizado por um sistema de refrigeração autônomo. Os pontos de interação definem as interfaces que permitem a comunicação e interação entre as diversas entidades envolvidas em algum processo do sistema. A partir disso, é possível identificar tanto o fluxo de dados no ambiente quanto as possíveis interfaces pelas quais um potencial atacante pode interagir com o ambiente IoT em análise.

4.3.3 Identificação do fluxo de dados

Esta atividade visa mapear o fluxo de dados da comunicação entre as entidades externas e/entre os componentes do ambiente IoT. O objetivo geral é identificar a comunicação e fluxo de dados entre as entidades. Um ponto de auxílio na identificação do fluxo de dados se dá pela utilização dos pontos de interação dos componentes do sistema. Assim, a partir dos pontos de interação, pode-se observar por quais componentes os dados devem trafegar, dado o *input* de usuários ou sistemas que interagem com estes componentes.

4.3.4 Identificação das tecnologias adotadas

A proposta desta atividade é identificar as diversas tecnologias que são utilizadas na implementação da solução proposta. Nesta atividade, deve-se olhar para cada componente e identificar quais tecnologias são utilizadas e implementadas para prover suas funcionalidades.

Neste ponto, deve-se identificar, por exemplo, fabricantes, sistemas operacionais, linguagens de desenvolvimento utilizadas, etc. Isto irá permitir identificar ameaças relacionadas a estas tecnologias específicas que são incorporadas como parte da solução. A identificação de tecnologias externas complementares auxilia em possíveis estratégias de *hardening* do ambiente.

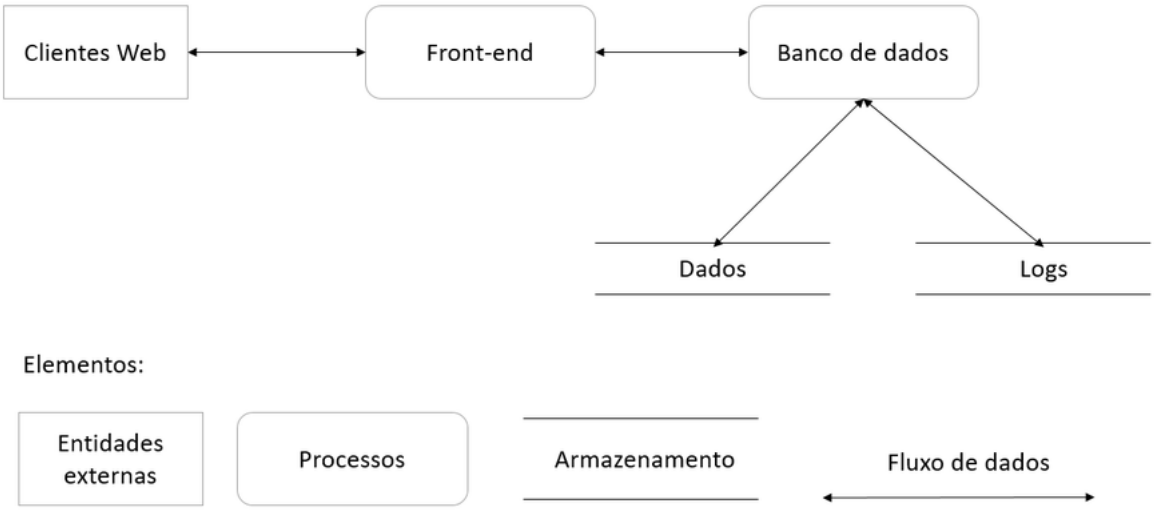
4.3.5 Criação do diagrama do ambiente

Após a coleta de informações das atividades anteriores, deve-se então criar um diagrama de representação da arquitetura do ambiente IoT estudado. Para isto, é recomendado utilizar uma notação formal e de fácil entendimento. Isto vai permitir a compreensão mais ampla das pessoas envolvidas no processo posterior de análise da arquitetura em busca de possíveis ameaças de segurança associadas ao sistema.

Dentre as principais técnicas utilizadas para a representação da visão arquitetural, temos o Diagrama de fluxo de dados (DFD), máquina de estados e representações através de UML. Para a metodologia proposta neste trabalho, o Diagrama de fluxo de Dados foi escolhido como a técnica de modelagem a ser utilizada por ser ter um foco em uma representação de alto nível do sistema, focando-se em como os dados são recebidos, como fluem dentre as diversas entidades em que o compõe e como são processados e armazenados. Complementarmente, esta técnica foi escolhida por ser usada como técnica de representação de sistemas na maioria dos trabalhos que foram utilizados como referência para o desenvolvimento desta pesquisa (MICROSOFT, 2003; OWASP, 2006).

Um exemplo da notação DFD utilizada para modelagem de arquiteturas de ambientes IoT, assim como sua notação, é mostrada na Figura 8:

Figura 8 – Exemplo de aplicação da notação DFD



Fonte: Produzido pelo autor

Onde:

- Entidades externas: representam um sistema, pessoas ou coisas que se comunicam com o sistema diagramado e que são origem ou destino de um fluxo de dados do sistema;
- Processos: representam qualquer processo que altere ou processe os dados, de forma a gerar uma saída;
- Armazenamento: indicam repositórios de armazenamento de dados do sistema;
- Fluxo de dados: representam o fluxo de dados entre as entidades externas, processos e repositórios de armazenamento do sistema diagramado.

4.4 Identificação de ameaças de segurança

A atividade de identificação de ameaças é o núcleo principal da modelagem de ameaças. É nesta fase que o ambiente será analisado em busca dos possíveis cenários de ameaças de segurança que estejam associados ao sistema IoT.

Este subprocesso se destina à identificação das possíveis ameaças de segurança do ambiente analisado. Como entrada, esta atividade do processo de modelagem recebe o diagrama de fluxo de dados gerado a partir das atividades anteriores. Como

saída, é gerada uma lista das ameaças de segurança associadas aos ativos do ambiente IoT.

Dentre os métodos utilizados para identificar ameaças de segurança que foram observados na literatura, existem *brainstorm*, a utilização de categorias de ameaças como o STRIDE (MICROSOFT, 2003; OWASP, 2006) e a geração automática de ameaças (SAITTA; LARCOM; EDDINGTON, 2005).

Contudo, como pontuado na seção de justificativa, as ameaças de segurança estão diretamente ligadas ao seu contexto. Por exemplo, as categorias de ameaça do STRIDE foram propostas considerando as principais características de ataques para o contexto de desenvolvimento de aplicações Web e, posteriormente, aplicações de software como um todo. Quando observamos o contexto da Internet das Coisas, é possível identificar categorias de ameaças que não podem ser representadas em sua totalidade através deste método. Por exemplo, ambientes baseados na Internet das Coisas podem ser compostos por dispositivos facilmente acessíveis fisicamente. Este fato viabiliza a introdução de ameaças que visem, por exemplo, a indisponibilidade do sistema através do acesso e dano físico a tais dispositivos.

Baseado no exemplo anterior, ataques que visassem danos físicos não encontrariam uma categoria correspondente no método proposto pelo STRIDE. Com isto, foi notada a dificuldade de migração e utilização direta do STRIDE para o contexto de IoT.

A partir desta observação, e baseado nos trabalhos de Nawir, Amir e Yaakob (2013) e Deogirikar e Vidhate (2017), os quais buscaram identificar ataques e a taxonomia de ataques voltados à Internet das Coisas, este trabalho buscou propor uma categorização de ameaças para IoT, com o intuito de auxiliar na identificação de ameaças direcionadas a este contexto. A partir do estudo realizado as categorias de ameaças físicas, ameaças de rede e ameaças de software foram propostas como método de categorização de ameaças para a Internet das Coisas. Tais categorias, suas descrições e as principais características de ataques que as compões são descritas a seguir.

4.4.1 Ameaças Físicas

A categoria de ameaças físicas caracteriza-se por ser composta por ataques diretamente direcionados aos *hardwares* que compõem o sistema. Nesta categoria de ameaças, os ataques podem ser divididos nas seguintes subcategoria:

- **Extração de informações sensíveis -** caracteriza-se por ataques onde um atacante tem acesso físico a um dispositivo que compõe a solução IoT com o objetivo de extrair informações sensíveis como, por exemplo, chaves de criptografia.

- **Adulteração do objeto -** conjunto de ataques onde um atacante visa adulterar as propriedades do dispositivo IoT, de forma a obter o controle do nó em questão. Através do acesso físico aos dispositivos, um atacante pode injetar códigos maliciosos que podem alterar o comportamento do nó comprometido em favor dos objetivos de um atacante. Por exemplo, um atacante pode redefinir um *firmware* de um dispositivo para uma versão comprometida, inclusão de *malwares*, *backdoors*, etc.

- **Negação de serviço -** compreendem ataques que visam tornar os serviços providos pelo sistema indisponíveis aos usuários legítimos. No contexto de ameaças físicas, um atacante pode causar danos físicos diretamente a uma coisa, tornando o sistema ou parte dos serviços do sistema indisponível;

- **Injeção de dispositivo malicioso -** inclui ataques onde um atacante adicione um nó malicioso ou substitua um nó (dispositivo/coisa) legítimo por um nó malicioso. Isto pode viabilizar, por exemplo, ataques *man-in-the-middle,* obtenção de informações sensíveis ou o comprometimento do sistema alvo.

4.4.2 Ameaças de Rede

Categoria de ameaças composta por ataques que visam explorar aspectos da rede utilizada pelo sistema IoT em análise. Os ataques de rede foram divididos nas subcategorias abaixo:

- **Análise de tráfego -** Esta categoria envolve tipos de ataques que visem interceptar o tráfego de comunicação de rede do sistema com a intenção de inferir padrões de comunicação e extrair informações sensíveis. Por exemplo, um atacante pode utilizar uma ferramenta de monitoramento de redes para analisar o tráfego de comunicação em busca de credenciais transmitidas em texto plano;

- **Falsificação de identidade -** Categoria que compreende ataques onde um atacante visa personificar um usuário ou entidades legítimas do sistema, através do roubo e utilização de seus atributos. Por exemplo, um atacante encaminha um pacote de rede para um computador do sistema com um endereço IP de origem indicando que este pacote é proveniente de uma entidade confiável. No contexto de IoT, ataques de falsificação podem envolver clone de *tags RFID*, repetição de tráfego interceptado, clones de endereço IP e man-in-the-middle;

- **Negação de serviço** - Categoria de ataques onde um atacante gera um alto tráfego de rede contra o sistema com a intenção de deixa-lo indisponível para os usuários legítimos. No contexto de ameaças de rede, um atacante pode, por exemplo, utilizar ferramentas de geração de tráfego automático para tentar tornar

indisponíveis os *sockets* de rede disponíveis para o estabelecimento de conexão, dada requisições de usuários legítimos;

- **Ataques contra criptografia -** Esta categoria envolve ataques que visem comprometer os mecanismos de criptografia utilizados na comunicação entre os componentes do sistema. Ataques desta categoria podem envolver, por exemplo, roubo de chaves privadas e a utilização de técnicas de criptoanálise.

4.4.3 Ameaças de Software

Categoria de ataques onde o atacante utiliza de artefatos de software para comprometer o sistema IoT. Os ataques dessa categoria podem ser observados principalmente pelo comprometimento dos ativos através de softwares maliciosos, mais conhecidos como *malwares.*

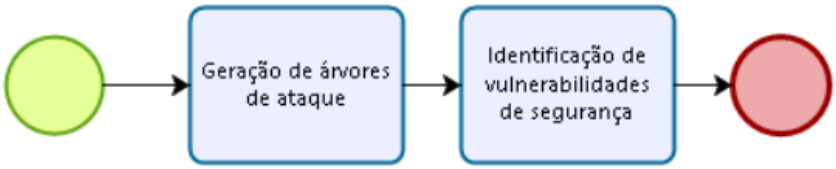
Um *malware* se refere a um *software* malicioso. Assim, esta categoria envolve ataques onde um atacante se utilize de dos diversos tipos de softwares maliciosos com o intuito de comprometer o sistema. Dentre os principais tipos de *malwares* pode-se citar: vírus, *worms*, *spywares*, cavalo de Tróia, *ramsonware,* dentre outros. *Malwares* podem ser utilizados para roubar informações sensíveis do sistema, prover interfaces de acesso (*backdoor*) ao atacante, esgotar recursos de rede e processamento, sequestro do sistema, etc. Por exemplo, um atacante, através da utilização de um *malware*, pode comprometer um dispositivo do sistema e torná-lo parte de uma *botnet*. Ou seja, uma rede de dispositivo comprometidos e sob o controle de um atacante.

4.5 Identificação de vulnerabilidades

Este subprocesso tem por objetivo identificar as vulnerabilidades que viabilizam as chances de sucesso do comprometimento do sistema IoT. Como explanado anteriormente, vulnerabilidades representam falhas de segurança que podem ser exploradas para concretizar um cenário de ameaça.

Para a identificação de vulnerabilidades de segurança, deve-se, primeiro, gerar as árvores de ataque para cada ameaça identificada e, a partir das árvores de ataque, realizar a análise e identificação das vulnerabilidades que viabilizam uma determinada ameaça.

Figura 9 – Atividades do subprocesso Identificar Vulnerabilidades



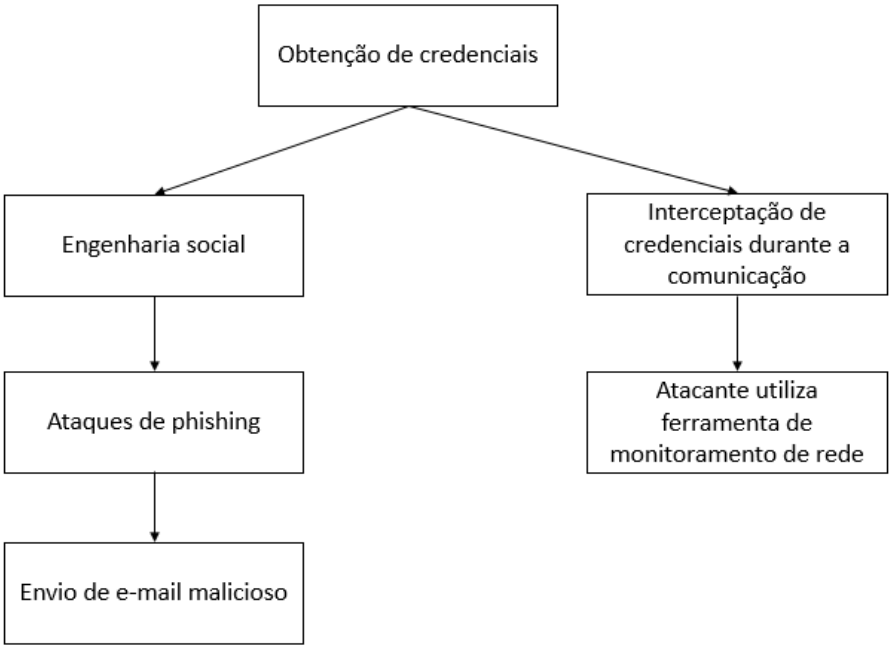
Fonte: Produzido pelo autor

4.5.1 Geração de árvores de ataque

Árvores de ataque fornecem uma estrutura formal e metódica para representar ataques contra um sistema (MICROSOFT, 2003). Assim, o nó raiz de uma árvore de ataque representa o objetivo de um atacante enquanto que os nós folhas representam os ataques que podem ser utilizados por um atacante para alcançar o seu objetivo principal. Durante o desenvolvimento de uma árvore de ataque também pode-se utilizar a notação *and* e or para representar possíveis relacionamentos entre ataque. Utilizar a notação *and,*significa que todas as condições associadas a este relacionamento precisam acontecer para que o objetivo de um atacante seja concretizado. Já a notação *or* indica que qualquer um dos vetores de ataque associados a este relacionamento precisa acontecer para que o objetivo de um atacante seja alcançado. Caso não haja nenhuma notação (*and* ou *or*) , isto significa, por padrão, uma condição *or .*

Uma árvore de ataque pode ser representada como mostrada na Figura 10:

Figura 10 – Exemplo de representação de árvore de ataque



Fonte: Produzido pelo autor

No exemplo anterior, o objetivo de um atacante seria obter as credenciais de acesso de um sistema. Neste exemplo, para conseguir tal objetivo, um atacante poderia se utilizar de dois ataques: interceptar credenciais de acesso durante o fluxo de comunicação e a utilização de técnicas de engenharia social.

Através de ferramentas de monitoramento de rede, um atacante poderia analisar o tráfego de comunicação entre os usuários e entidades do sistema, visando capturar alguma credencial passada em texto plano.

Em um outro ataque, um atacante poderia se utilizar de técnicas de engenharia social como *phishing* ou personificação de uma pessoa ou entidade confiável para obter as credenciais do usuário. Dentre os exemplos de ataque de *phishing*, um atacante pode enviar e-mails contendo *malwares* que visem comprometer o sistema e capturar a senha do usuário alvo.

A geração de árvores de ataque permite a identificação das vulnerabilidades que viabilizam o cenário de ameaça, representado pelo objetivo do atacante. A partir da identificação de vulnerabilidades é possível então compreender quais vulnerabilidades precisam ser mitigadas para reduzir as probabilidades da concretização da ameaça em questão.

4.5.2 Identificação de Vulnerabilidades de segurança

A partir dos vetores de ataque presentes nas árvores de ameaça, deve-se identificar as possíveis fraquezas que viabilizam suas chances de sucesso. A identificação das vulnerabilidades associadas as ameaças fornecem insumos para a proposição de contramedidas de segurança que visem diminuir a probabilidade de exploração de um determinado sistema através de um determinado vetor de ataque.

Por exemplo, tomando como referência a árvore de ataque descrita na Figura 11, o objetivo define-se pela obtenção de credenciais de acesso ao sistema. Para isso, os vetores de ataque presente na árvore de ataque apontam que, para que esta ameaça seja possível, as credenciais de acesso devem ser enviadas sem a utilização de nenhum mecanismo de criptografia (em texto plano) e o atacante, através da utilização de ferramentas de monitoramento de rede, consegue identificar credenciais trafegadas em texto plano. Embora seja um exemplo simples, este cenário nos permite identificar que a vulnerabilidade que viabiliza a concretização do cenário de ameaça é o envio de credenciais em texto plano. Ou seja, a não utilização de mecanismos de criptografia para a comunicação entre ambas as partes envolvidas permite que um atacante obtenha com sucesso as credenciais de acesso ao sistema.

A proposição das medidas de segurança deve ser feita pela equipe técnica responsável pela análise do modelo de ameaças produzido por esta metodologia. Contudo, vale salientar que esta metodologia, em seu estado atual, não visa a proposição de contramedidas de segurança e sim prover insumos para viabilizar a proposição dessas contramedidas.

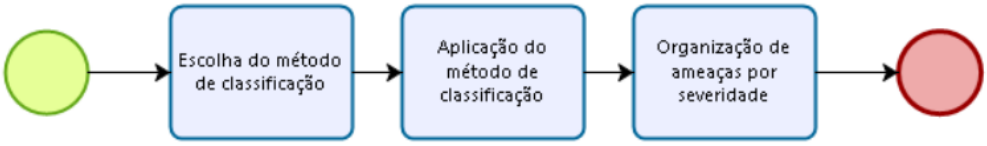
4.6 Classificação de Ameaças

Com os insumos fornecidos pela identificação das ameaças de segurança associadas ao diagrama arquitetural de alto nível do sistema, as próximas atividades no processo de modelagem referem-se à classificação destas ameaças. Em outras palavras, as atividades de subprocesso destinam-se a atribuições do risco associado a cada ameaça registrada e a sua devida organização a partir de seu atributo de risco.

Como tratado nas seções de justificativa e trabalhos relacionados, o método de classificação DREAD foi escolhido como o mais completo no que se refere ao conjunto de propriedades consideradas no processo de cálculo do risco de uma ameaça. Contudo, as propriedades que compõem este método estão associadas as ameaças do contexto de aplicações de *software*. Com isto, foi observada a necessidade de adaptação de suas propriedades para considerar a sua aplicabilidade ao contexto de IoT.

Partindo deste princípio, através da revisão da literatura, observou-se que o trabalho proposto por Sándor e Sebestyén-Pál (2017), também apresentado no capítulo de trabalhos relacionados, realizou uma adaptação inicial deste sistema classificação para o contexto de IoT. Baseado no trabalho realizado por estes pesquisadores, este trabalho propõe uma extensão do seu sistema de classificação, o qual pode ser consultado na seção 4.5.1 correspondentes à escolha do método de classificação. A Figura 11 mostra a representação das atividades deste subprocesso:

Figura 11 – Atividades do subprocesso de Classificação de Ameaças



Fonte: Produzido pelo autor

4.6.1 Escolha do Método de Classificação de ameaças

Esta atividade define a especificação do método de classificação de ameaças. Como abordado na seção 4.5, este trabalho apresenta uma contribuição no que concerne à extensão do método de classificação DREAD aplicado a IoT no trabalho de Sándor e Sebestyén-Pál (2017). Como principais modificações realizadas no esquema de classificação, este trabalho procurou dividir a propriedade *Affected* em duas categorias distintas.

No trabalho proposto por Sándor e Sebestyén-Pál (2017), esta propriedade considerava os aspectos do quanto uma ameaça afetava usuários ou coisas como uma métrica única. Contudo, este trabalho considera que a gravidade na qual uma ameaça afeta um usuário ou um grupo de usuários não depende diretamente da quantidade de coisas afetadas no sistema.

A partir deste raciocínio, este trabalho dividiu esta propriedade, procurando identificar a gravidade na qual uma ameaça afeta os usuários do sistema e a quantidade de coisas comprometidas no ambiente sob análise. Os parâmetros e descrições modificados encontram-se com seus campos sinalizados com o caractere '*'. Com isto, o esquema de classificação proposto é apresentado na Tabela 3:

Tabela 3 – Esquema de classificação estendido para IoT

Classes	Muito baixo* (0)	Baixo (1)	Médio (2)	Alto(3)
Damage	Atividade sem nenhum dano	Vazamento trivial de informações acerca do ativo IoT e/ou usuários	Vazamento de informação sensível acerca do coisas e/ou usuários, ou perda de qualquer tipo de informação	Permite que um atacante comande um dispositivo IoT obtenha total autorização, execute com privilégios administrativos
Reproducibility	Para o componente afetado, existe mecanismos de proteção disponíveis contra o ataque	O ataque é difícil ou impossível de reproduzir	O ataque apenas pode ser reproduzido com uma janela de tempo específica e uma condição de corrida particular	O ataque pode ser reproduzido a qualquer momento
Exploitability	Mesmo que haja probabilidades estatísticas de exploração, o ataque requer diversos recursos que por sua vez são probabilisticamente menos disponíveis	O ataque requer uma pessoa com profundo conhecimento técnico ou com conhecimento interno do sistema todas as vezes para realizar a exploração	Uma pessoa tecnicamente hábil, como um programador, pode realizar o ataque e, posteriormente, repetir os passos de exploração	Um programador iniciante ou pessoas sem conhecimento técnico pode realizar o ataque em tempo hábil seguindo um guia

Classes	Muito baixo* (0)	Baixo (1)	Médio (2)	Alto(3)
**Affected Things*	* O ataque não afeta nenhuma coisa	*Um pequeno número coisas são afetadas	* Um grupo, por exemplo, subdomínio, de coisas são afetadas	*Todos as coisas são afetadas
**Affected Users*	*A ameaça não põe em risco de vida ou danos diretos aos usuários do sistema IoT	* A ameaça fornece baixo risco de vida e/ou danos diretos aos usuários do sistema IoT	* A ameaça oferece risco de vida e/ou danos diretos consideráveis aos usuários do sistema IoT	* Alto risco de vida e/ou danos diretos aos usuários do sistema IoT
Discoverability	Uma solução alternativa é aplicada que corrige a vulnerabilidade	A vulnerabilidade tem comportamento difícil de ser entendido. Portanto, é muito difícil compreender os possíveis danos potenciais de sua exploração	A vulnerabilidade pode ser acessada por apenas alguns usuários e seria necessário esforço para enxergar o uso malicioso	Guias publicados são disponíveis para ataque ou a vulnerabilidade é visível ou facilmente perceptível através da interface do usuário

Fonte: Produzido pelo autor

A partir das propriedades descritas na tabela anterior, deve-se somar os valores atribuídos a cada uma delas e dividir o total por seis. Este cálculo resultará, enfim, no risco que será atribuído a uma ameaça.

Adicionalmente, alguns outros métodos de classificação de ameaças podem ser utilizados. São estes: *Risk = probability * damage potential* ou a atribuição dos valores de *High, Medium* ou *Low*.

4.6.2 Aplicação do método de classificação

Após a definição do método de classificação a ser utilizado, deve-se aplicar este método a cada ameaça identificada. A saída esperada desta atividade são todas as ameaças associadas aos seus respectivos riscos.

4.6.3 Organização de ameaças por severidade

Após a aplicação do método de classificação, se faz necessário organizar as ameaças por severidade. O intuito desta atividade é desenvolver um ranking de ameaças baseado em seus riscos associados. Para isto, basta organizar as ameaças identificadas a partir da ameaça com maior risco para a ameaça de menor risco. Isto permitirá, por exemplo, a visão das ameaças das mais críticas para as menos críticas. A partir desta visão, é possível priorizar os esforços de segurança na remediação e mitigação das ameaças mais críticas.

4.7 Documentação de artefatos

A última fase do processo de modelagem refere-se à documentação dos principais artefatos gerados durante todas as atividades. A documentação destes artefatos serve de referência técnica e facilitam o processo de consulta do que foi produzido após a aplicação da metodologia.

Tais artefatos podem ser organizados e documentados de forma a serem apresentados como um relatório técnico. A documentação gerada pela saída do processo de modelagem de ameaças de segurança aplicável a IoT é referenciada como um modelo de ameaças.

Para o contexto deste trabalho, um modelo de ameaça é formado pelo conjunto dos seguintes artefatos: diagrama de fluxo de dados, ameaças de segurança identificadas, árvores de ataque, vulnerabilidades, classificação ameaças e *ranking* de ameaças. Assim, a documentação de todos estes artefatos compõe o modelo de ameaças final do sistema IoT analisado e encerra o processo de modelagem de ameaças de segurança.

4.8 Saída geral do processo

Após a execução das atividades de modelagem, a saída esperada é o artefato definido como modelo de ameaças. O modelo de ameaças é composto pela visão arquitetural de alto nível do sistema, a lista de ameaças de segurança identificadas, os vetores de ataque utilizados para atingir cada objetivo das ameaças, as vulnerabilidades que viabilizam os ataques, a classificação das ameaças e sua consequente organização pelos seus respectivos riscos.

5 Estudo de caso

Com o intuito de avaliar a metodologia proposta, este trabalho realizou um estudo de caso, onde buscou-se aplicar a abordagem de modelagem de ameaças de segurança em ambientes IoT ao sistema IoT proposto no trabalho de Piyare (2013). O ambiente utilizado para o estudo de caso foi escolhido por se enquadrar em um dos principais domínios de aplicações da Internet das Coisas (casas inteligentes), por ser um trabalho de referência e por prover insumos suficientes para a aplicação da metodologia proposta. Além da descrição técnica do sistema sob análise, este capítulo também apresenta a aplicação de cada etapa da modelagem de ameaças proposta neste trabalho ao ambiente IoT analisado. Adicionalmente, considerações sobre resultados e discussões são realizadas ao fim do capítulo.

5.1 Estudo de caso: Sistema de controle e monitoramento doméstico utilizando smartphone

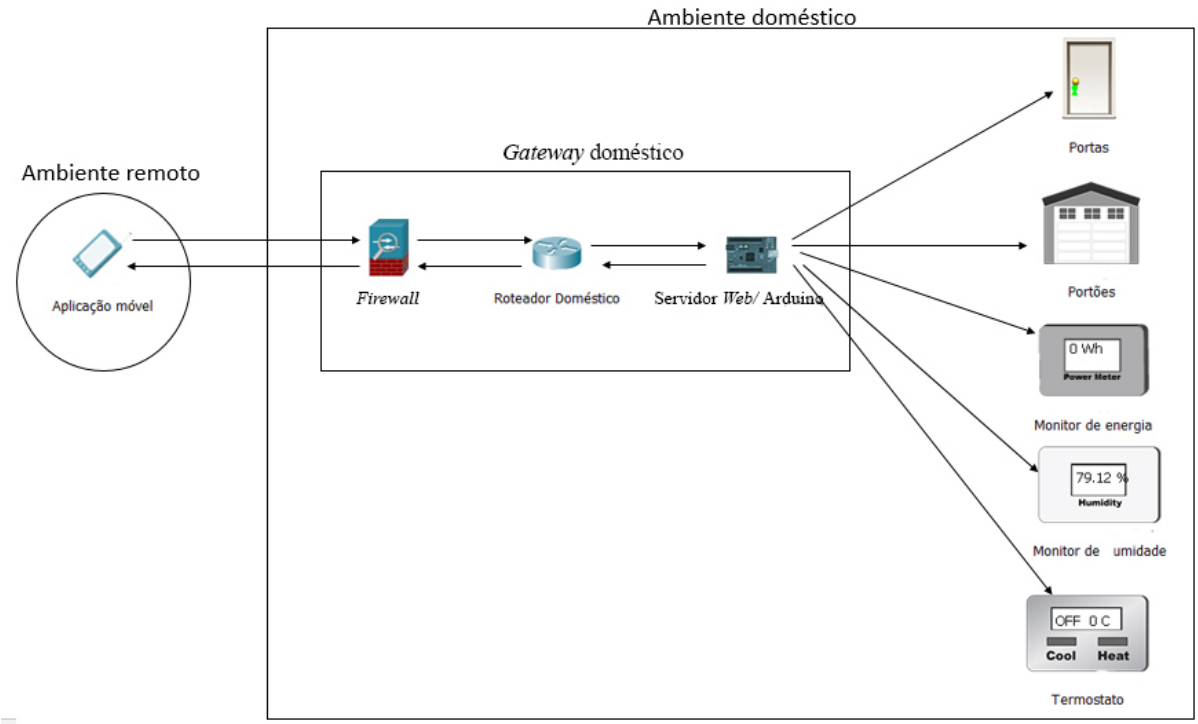
5.1.1 Visão geral do sistema

O sistema escolhido como estudo de caso apresenta uma aplicação de baixo custo para o controle e gerenciamento remoto de casas inteligentes através da utilização de *smartphones* que utilizam o sistema Android.

O núcleo do sistema se baseia em um micro *Web* server sendo executado em um Arduino (PIYARE, 2013). O servidor *Web* provê o conjunto de serviços de controle e monitoramento através uma API REST, acessível através de um *client* baseado em uma aplicação voltada a dispositivos que utilizam o sistema Android.

A partir dos comandos recebidos através da API REST, o dispositivo central é responsável por executar o controle e gerenciamento dos dispositivos periféricos como: sensor de temperatura, sensor e controlador de umidade, luzes, fechaduras e tomadas de energia. A representação do sistema pode ser melhor compreendida a partir da Figura 12:

Figura 12 – Visão Geral do cenário adotado no Estudo de Caso



Fonte: Produzido pelo autor

5.1.2 Principais funcionalidades

A partir da aplicação móvel provida pelo sistema, o servidor *web* fornece as seguintes funcionalidades:

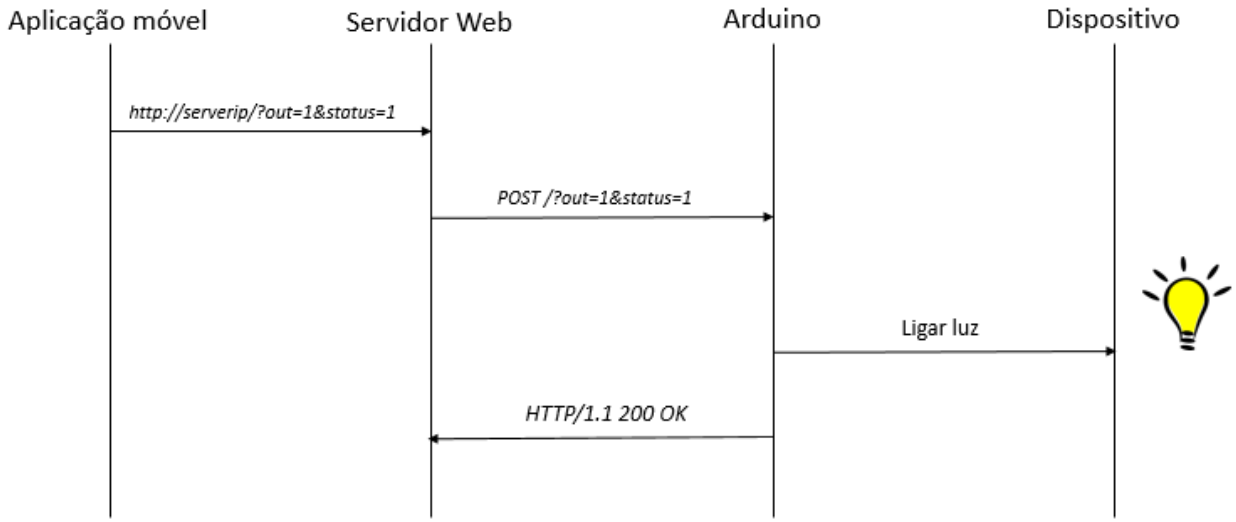
- Conexão remota com o *gateway* doméstico (tradução livre de *home gateway*);
- Controle de dispositivos;
- Monitoramento de dispositivos;
- Agendamento de gerenciamento.

Para a realização da conexão com o servidor web, o usuário apenas necessita configurar o endereço IP e porta na qual o servidor disponibiliza os serviços do sistema. Para recuperar os dispositivos conectados ao Arduino e disponíveis para as operações de controle e gerenciamento, a aplicação envia uma requisição no formato: http://<ip-web-server>/?out=all e como retorno, a aplicação recebe, por exemplo, um JSON no seguinte formato: {“ip” : “endereço ip”, “devices” :[{ “type” : “light”, “name” : “Light 1”, “out” : “5”},{ “type” : “light”, “name” : “Light 2”, “out” : “6”},{ “type” : “temperature”, “name” : “Temperature sensor”, “out” : “7”},{ “type” : “plug”, “name” : “Power Plug”, “out” :

“8”},{ “type” : “door”, “name” : “Front Door”, “out” : “9”},{ “type” : “gate”, “name” : “Main Gate”, “out” : “10”},{ “type” : “wattmeter”, “name” : “Main Switch Board”, “out” : “2”}]}.

De forma geral, o sistema retorna o endereço IP do servidor e uma lista contendo os dispositivos disponíveis. 13Sobre os dispositivos, o JSON retornado pelo servidor contém informações sobre o tipo do dispositivo, o nome e porta na qual o dispositivo está conectado ao Arduino, a qual é utilizada para as operações de controle e gerenciamento. Um exemplo de uma operação de controle de dispositivo através do serviço provido pelo sistema é mostrado na Figura 13:

Figura 13 – Exemplo de fluxo de comunicação



Fonte: Produzido pelo autor

Neste exemplo, a aplicação móvel envia a requisição ao servidor *Web*, especificando qual a porta correspondente ao dispositivo e a ação a ser tomada (neste caso, acender a luz conectada à porta 1). Ao receber a requisição, o servidor *Web* processa a mensagem recebida e solicita a operação requisitada pelo usuário, confirmando a operação através uma mensagem HTTP 200 OK.

5.2 Aplicação da metodologia de modelagem de ameaças

5.2.1 Modelagem da arquitetura do ambiente

As atividades a seguir correspondem a primeira fase da modelagem de ameaças de segurança em ambientes IoT. Nesta atividade, foram coletados insumos a respeito

do sistema, suas principais funcionalidades e arquitetura, com o intuito de gerar como saída um diagrama de fluxo de dados que representa a visão arquitetural do sistema sob análise.

5.2.1.1 Identificação de componentes do sistema

Os principais ativos que compõem a solução IoT apresentada por este sistema são:

- Arduino Uno ATMEGA 328;
- Aplicação móvel JAVA utilizada como cliente de controle e gerenciamento;
- API REST;
- Sensor de temperatura LM35;
- Sensor de 30A para monitoramento de energia;
- Lâmpadas;
- Fechaduras de portas/portões;
- Tomadas de energia.

5.2.1.2 Identificação de pontos de interação com o sistema

Pontos de interação definem as interfaces pelas quais o sistema pode ser acessível por um usuário e, consequentemente, por um potencial atacante. Para o sistema em análise foram identificados os seguintes pontos de interação:

- Aplicação JAVA utilizada como *client* em dispositivos baseados em android, desenvolvida através do Android Software Development Kit (SDK);
- API REST em execução no servidor *Web*.

A aplicação móvel desenvolvida para smartphones Android apresenta-se como um ponto de interação pois, a partir desta aplicação, é possível utilizar das funcionalidades de controle e gerenciamento do sistema. As requisições enviadas pela aplicação móvel são processadas pela API e executadas diretamente no ambiente da casa inteligente.

A API REST é responsável por fornecer a interface entre os usuários e o ambiente do sistema, viabilizando as funcionalidades disponíveis do sistema, sendo esta a principal responsável pelo recebimento e processamento das requisições dos usuários do sistema.

5.2.1.3 Identificação de fluxo de dados

A partir dos ativos que compõem o ambiente analisado, as seguintes informações sobre o fluxo de dados foram mapeadaa:

Tabela 4 – Fluxo de dados entre os componentes do sistema

Ativo	Componentes com o qual se comunica
Aplicação móvel	*Gateway* doméstico, composto pelo *firewall*, roteador e API (servidor *Web*)
Firewall	Aplicação móvel e roteador doméstico
Roteador domético	Firewall e servidor Web/Arduino
Servidor Web	Roteador doméstico e dispositivos gerenciados

Fonte: Produzido pelo autor

Tais informações serão utilizadas e representadas na seção 5.2.1, correspondente a atividade de modelagem da arquitetura do ambiente.

5.2.1.4 Identificação de tecnologias adotadas

Como principais tecnologias adotadas como parte da solução do sistema proposto, pode-se citar:

- Linguagem JAVA, utilizada no desenvolvimento da aplicação usada como *client*;
- Sistema Android, o qual irá ser responsável por executar a aplicação *client;*
- API REST em execução no servidor *Web*;
- Arduino Uno.

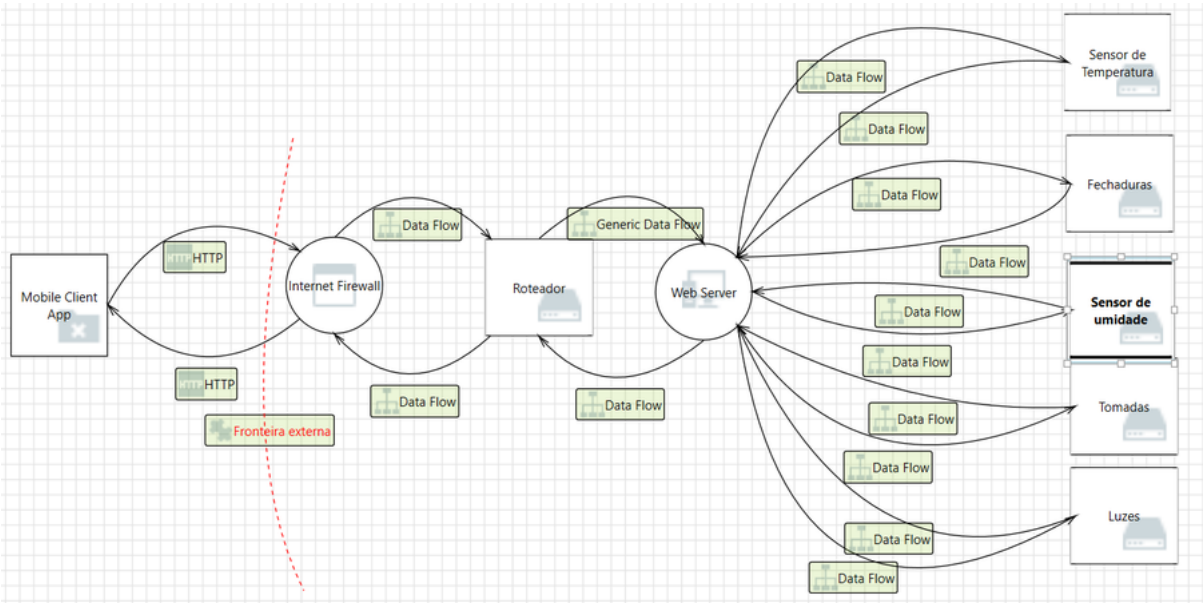
As tecnologias identificadas são utilizadas para viabilizar a execução do sistema principal. Contudo, essas tecnologias podem ser alvo de suas próprias vulnerabilidades, que podem eventualmente serem exploradas, servindo como vetor de ataque do sistema principal. Com isso, a identificação das tecnologias citadas serve de insumos para possíveis estratégias de *hardening* do ambiente. Para maiores detalhes sobre a implementação do trabalho utilizado no estudo de caso é possível consultar o trabalho proposto por Piyare (2013), do qual as especificações foram extraídas.

5.2.1.5 Criação do diagrama do ambiente

A partir dos insumos identificados e coletados nas fases anteriores, um diagrama de fluxo de dados foi criado. O diagrama representa a visão arquitetural de alto nível do sistema, destacando seus principais componentes, fluxo de dados e fronteiras de confiança.

Para a realização da criação do diagrama foi utilizada a ferramenta Threat Modeling Tool 2016 (MICROSOFT, 2016) . O DFD que representa o fluxo de dados do sistema está especificado na Figura 14:

Figura 14 – Modelagem do diagrama de fluxo de dados do sistema



Fonte: Produzido pelo autor.

5.2.2 Identificação de ameaças de segurança

Nesta seção serão apresentados os resultados das atividades do subprocesso da etapa de identificação de ameaças do sistema. A atividade de identificação de ameaças é o núcleo da modelagem de ameaças. Nesta etapa, o diagrama arquitetural do sistema foi analisado e os principais cenários de ameaça foram identificados. São estes:

- **Danos Financeiros** – Um atacante pode causar danos financeiros aos usuários do sistema através do aumento do consumo energético causado pela manipulação dos componentes periféricos do ambiente. Por exemplo, enquanto os usuários não se encontram na residência, um atacante pode ligar luzes ou periféricos que aumentem o consumo energético total da residência, resultando em um aumento do custo total da fatura energética aos usuários ;

- **Danos à saúde dos usuários** – Um atacante pode causar danos à saúde dos usuários através da manipulação dos componentes que controlam e gerenciam variáveis de ambiente como temperatura e umidade. Por exemplo, através da variação constante de parâmetros de temperatura e umidade do ambiente, um atacante pode desencadear complicações de saúdes aos residentes (DUNCAN; FELLOUS; KALTZ, 2013);

- **Sequestro de usuários** – Em um cenário mais extremo, através do comprometimento do sistema IoT em análise, um atacante poderia ter acesso à residência dos usuários através do controle dos dispositivos responsáveis pela segurança da residência. Com isto, um atacante poderia realizar ações que colocassem em risco direto a vida dos residentes. Por exemplo, desde danos físicos até sequestros de residentes;

- **Roubo residencial** - Através do comprometimento do sistema IoT em análise, um atacante poderia ter acesso à residência dos usuários com a intenção de roubar patrimônios físicos contidos na residência;

- **Negação de serviço –** Um atacante pode tornar o sistema indisponível através de ataques de negação de serviço que visem impossibilitar que usuários legítimos tenham acesso aos serviços disponibilizados pela API do servidor *Web*;

- **Espionagem da rotina dos usuários -** Ferindo princípios de privacidade, um atacante poderia obter insumos sobre a rotina dos usuários do sistema através da utilização de técnicas de análise de tráfego. Por exemplo, um atacante poderia tentar inferir os horários de maior ou menor presença de pessoas na residência, os quais poderiam servir de insumo para cenários de ameaça posteriores como roubo residencial, sequestro, suborno, etc;

- **Botnet –** Um atacante pode explorar o sistema IoT com o intuito de utilizar os recursos computacionais do sistema como parte de uma rede de computadores sob o seu controle. Com isto, o atacante pode se utilizar desses recursos computacionais para, por exemplo, executar ataques em outras redes, para o processamento de dados, etc.

5.2.3 Identificação de Vulnerabilidades

A seguir, serão apresentados os resultados da etapa de identificação de vulnerabilidade para o sistema analisado.

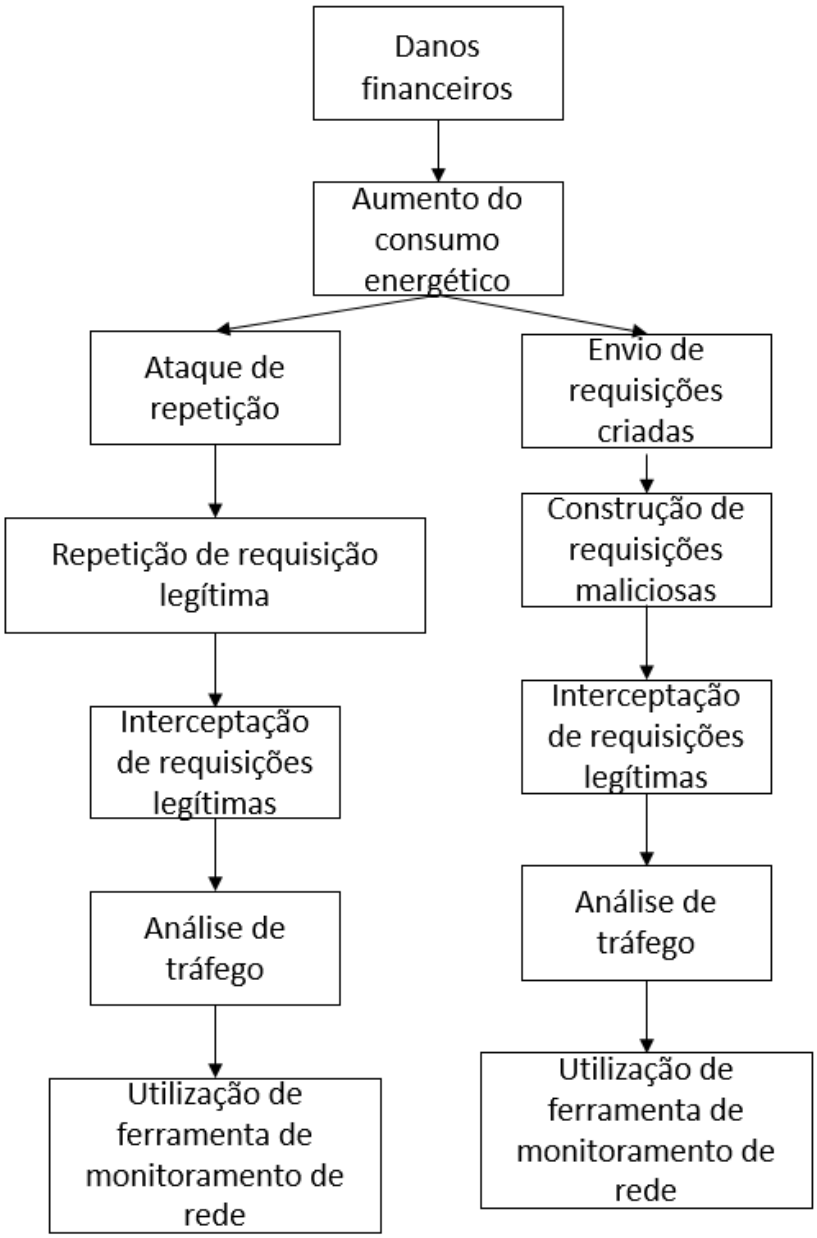
5.2.3.1 Geração de Árvores de Ataque

Esta subseção apresenta as árvores de ameaça geradas a partir das ameaças associadas ao sistema IoT, as quais foram apontados na fase de identificação de ameaças.

Ameaça de danos financeiros representa a intenção de um atacante de realizar danos financeiros aos usuários do sistema através do aumento do consumo energético da residência na qual o sistema IoT é responsável por controlar e gerenciar. Dentre os componentes que podem ser manipulados através do sistema, encontram-se lâmpadas, tomadas de energia e componentes que poderiam ser utilizados para gerar um maior consumo energético da residência, visando resultar em danos financeiros aos seus usuários.

A Figura 16 representa a árvore de ataque de ataque que descreve os possíveis vetores de ataque que podem ser utilizados por um atacante para alcançar este objetivo:

Figura 15 – Árvore de ataque para ameaça de danos financeiros



Fonte: Produzido pelo autor

A partir da representação da ameaça, é possível verificar que, para chegar a este objetivo, um atacante pode se utilizar de dois vetores de ataque distintos: utilizar ataques de repetição (tradução livre de *replay attacks*) e o envio de requisições criadas.

Ataques de repetição ocorrem quando um atacante consegue interceptar um fluxo de mensagens legítimo entre as partes envolvidas e o repete posteriormente. Caso não haja nenhum mecanismo de mitigação, o mesmo fluxo de comunicação pode ser processado por uma das partes para a realização de atividades maliciosas como um usuário legítimo do sistema.

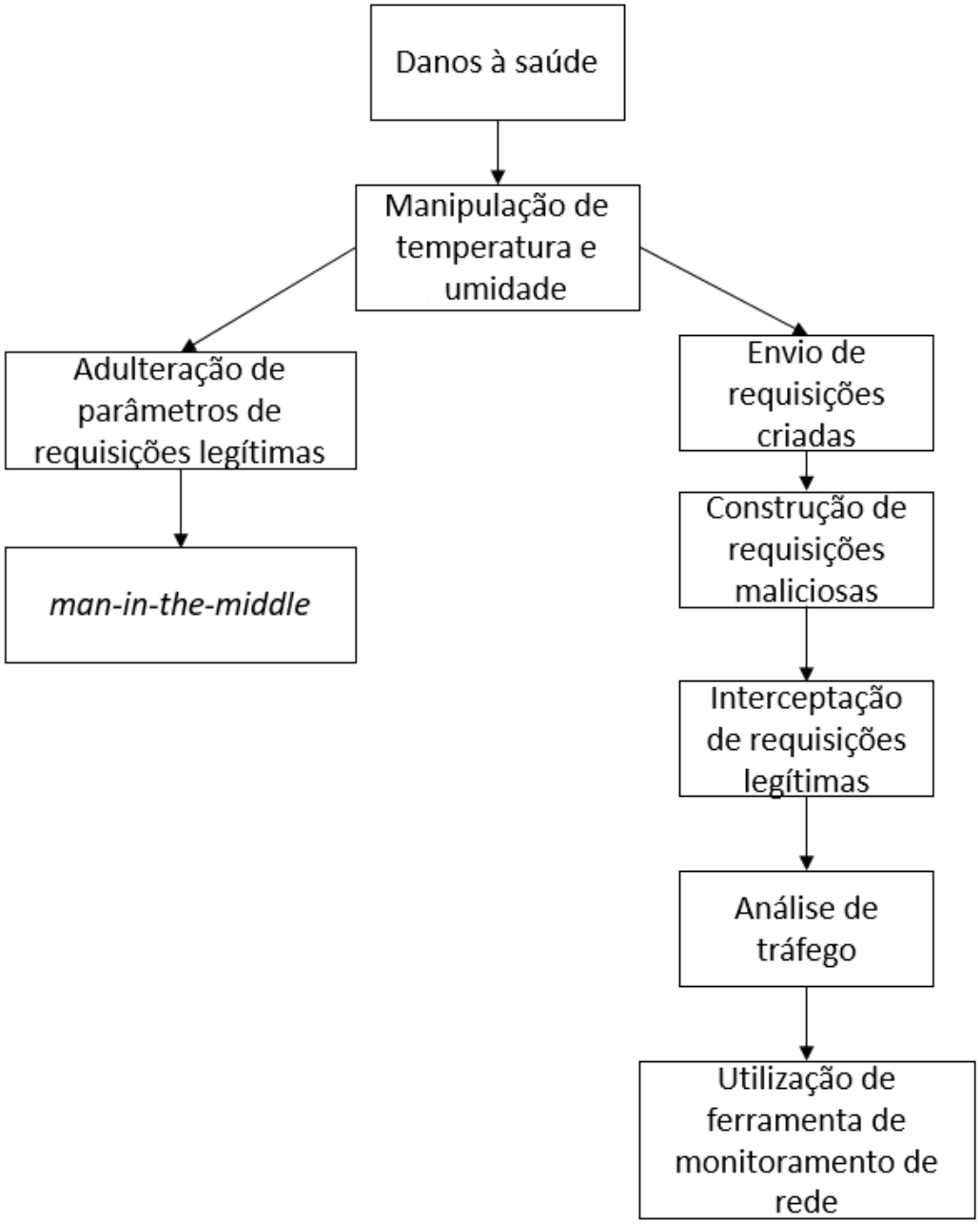
No cenário do sistema sob análise, um atacante pode se utilizar de ferramentas

de monitoramento de rede para tentar identificar um fluxo de comunicação entre o cliente e o servidor *Web* responsável pelo controle e gerenciamento da residência inteligente. Ao identificar e interceptar uma requisição legítima, levando em consideração que o servidor *Web* não utiliza nenhum mecanismo de autenticação, um atacante poderia então repetir esta requisição e executar comandos válidos no sistema. Por exemplo, um atacante poderia utilizar a requisição interceptada para acender luzes, ativar sensores e outros dispositivos controlados pelo sistema. Isto, então, resultaria num maior consumo energético, o que levaria a concretização do cenário deste cenário de ameaça.

Já através do vetor de ataque representado pelo envio de requisições criadas, a técnica utilizada por um atacante seria similar ao cenário de ataques de repetição. Contudo, ao invés de apenas repetir o mesmo fluxo comunicação interceptado, um atacante poderia customizar a requisição para personalizar as ações maliciosas a serem executadas no sistema.

Para o cenário da ameaça de danos à saúde, a árvore de ataques correspondente pode ser compreendida pela Figura 16:

Figura 16 – Árvore de ataque para ameaça de danos à saúde



Fonte: Produzido pelo autor.

A árvore de ataque para danos à saúde se assemelha ao cenário da árvore de ataque descrita para a árvore de dano financeiro, onde um atacante se utiliza de requisições criadas e da ausência de mecanismos de autenticação entre a comunicação entre o cliente e o servidor do sistema para executar comandos do sistema.

Para este cenário de ameaça, após a interceptação e identificação de um fluxo de dados legítimo, um atacante poderia personalizar as ações maliciosas a serem executadas no sistema. Neste caso, um atacante poderia manipular variáveis como

temperatura e umidade residencial, com o intuito de provocar complicações de saúde aos usuários e moradores da casa inteligente.

Adicionalmente, um atacante poderia manipular e adulterar as requisições vindas dos usuários. Neste caso, o atacante poderia realizar um ataque *man-in-the-middle*. Ou seja, personificar tanto o servidor para um cliente que faz uma requisição, quanto um usuário legítimo para o servidor que recebe esta requisição. Com isto, dada as requisições advindas de um usuário, um atacante poderia interceptar e manipular conforme seu objetivo.

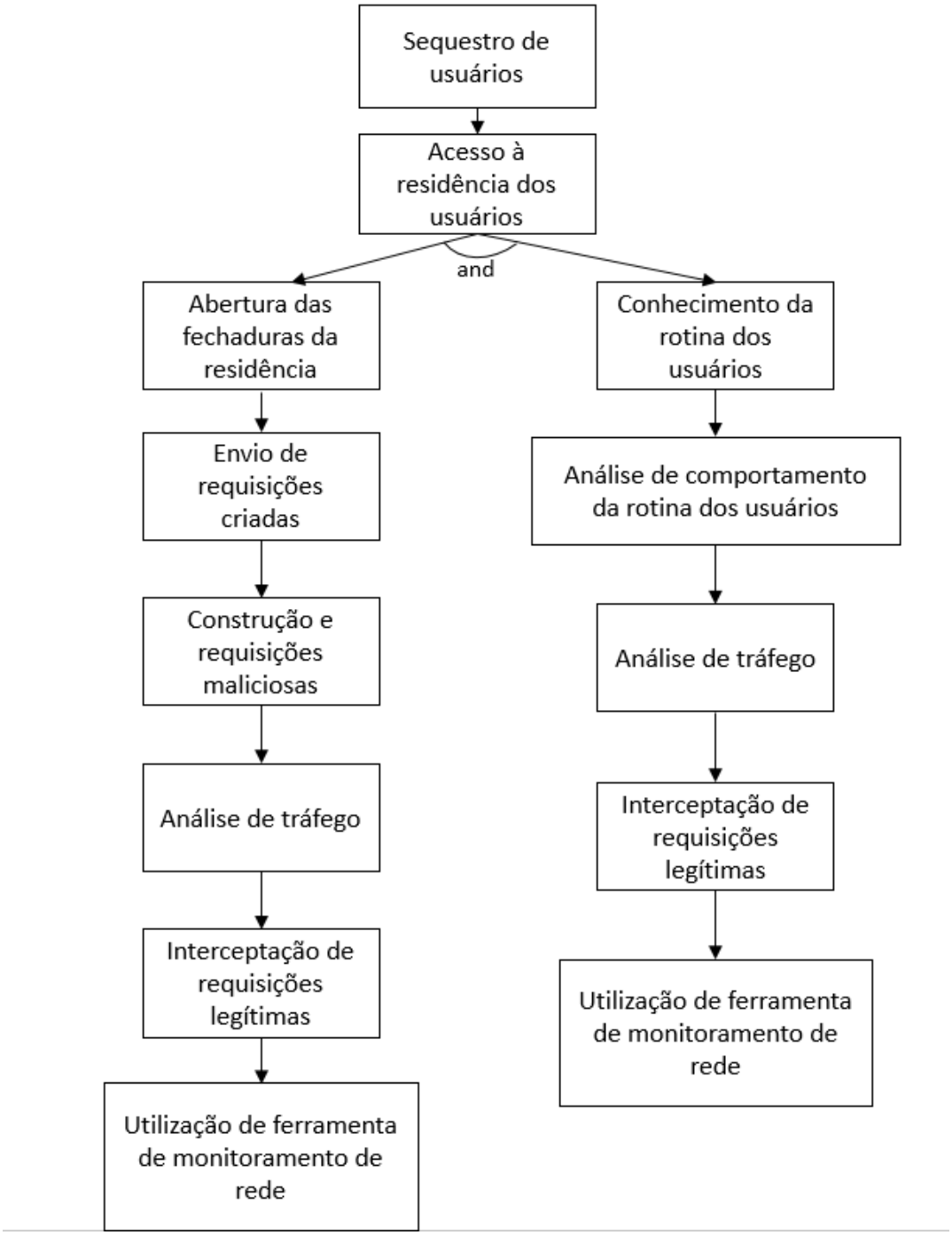
Em um cenário de ameaças onde um atacante vise sequestrar os usuários (residentes), se faz necessário que ele tenha acesso a residência. Para isto, um atacante precisa manipular o sistema para abrir as fechaduras controladas pelo servidor, em conjunto com o conhecimento da rotina dos residentes.

Para alcança o objetivo de manipular a abertura das fechaduras controladas pelo sistema IoT, um atacante precisa seguir os mesmos passos citados anteriormente para a criação/construção de requisições maliciosas, já descritos nas árvores de ataques anteriores.

Em conjunto com a capacidade de manipulação do sistema através da execução de requisições maliciosas, um atacante necessita inferir a rotina dos usuários para a maior efetividade de sua ação. Para isto, um atacante poderia realizar uma análise comportamental da rotina dos usuários, baseado na interceptação das requisições feitas para o sistema, se utilizando de ferramentas de monitoramento de rede. A realização desses ataques aumentaria, assim, a probabilidade de sucesso da concretização deste cenário de ameaça.

A imagem a seguir demonstra a descrição da árvore de ataque para este cenário de ameaça:

Figura 17 – Árvore de ataque para ameaça de sequestro de usuários



Fonte: Produzido pelo autor

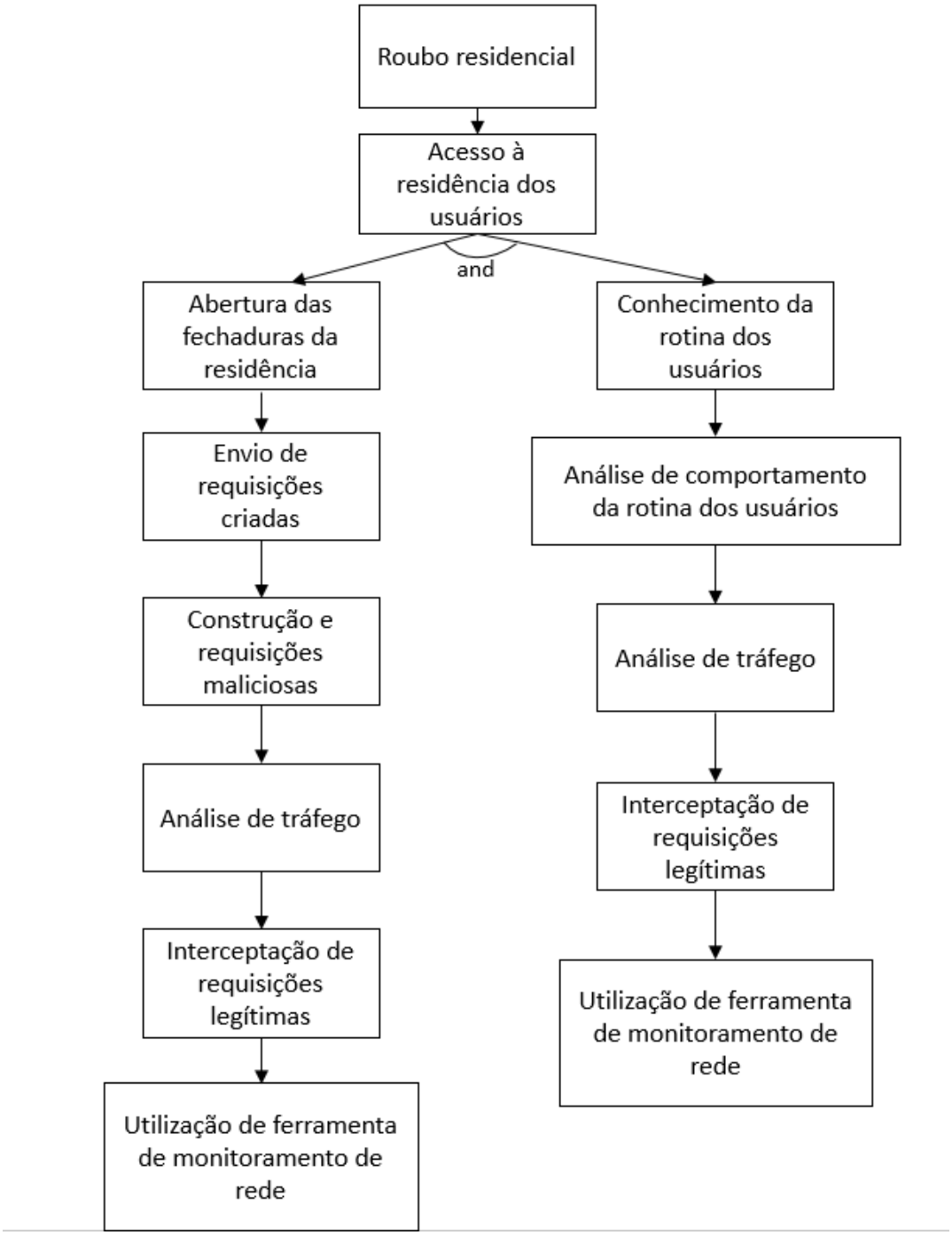
O processo para que o cenário de roubo residencial ocorra é similar ao de sequestro de usuários. Em outras palavras, se faz necessário que um atacante seja capaz de criar requisições maliciosas, as quais se baseiam em requisições legítimas que foram interceptadas, que são recebidas e executadas como a de um usuário legítimo pois não existem mecanismos de autenticação implantados do servidor.

Em conjunto com este vetor, um atacante necessita do conhecimento da rotina

dos residentes, que pode ser obtida a partir da análise comportamental da rotina dos usuários, baseada na interceptação e análise de tráfego da comunicação entre o cliente e o servidor.

Este cenário é representado na Figura 18:

Figura 18 – Árvore de ataque para ameaça de roubo residencial



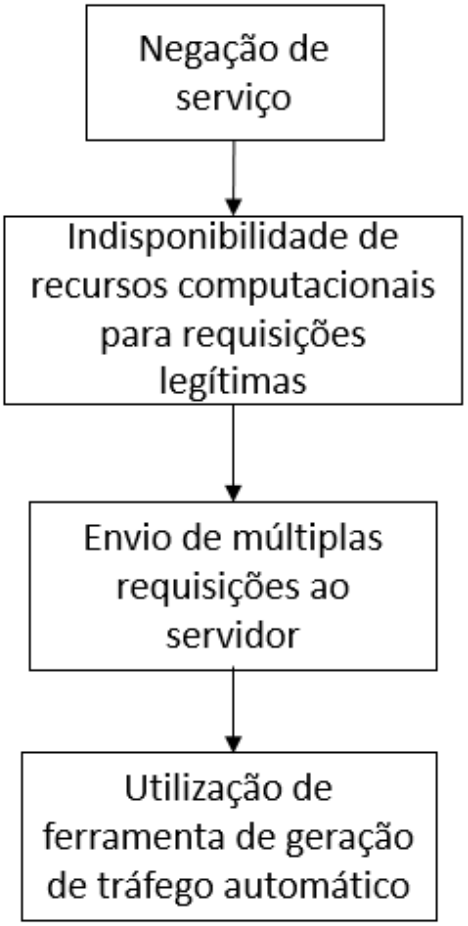
Fonte: Produzido pelo autor

Ataques de negação de serviço visam comprometer a disponibilidade do sistema para usuários ou requisições legítimas. Por exemplo, um atacante pode visar esgotar

os *sockets* de rede disponíveis para o estabelecimento de conexões legítimas ou o esgotamento de recursos de memória ou processamento.

No cenário analisado, um atacante poderia se utilizar de ferramentas de geração de tráfego automatizado para visar o comprometimento da disponibilidade do sistema. O envio de múltiplas requisições poderia resultar no esgotamento dos *sockets* de rede disponíveis para o estabelecimento de novas requisições, tornando o servidor web indisponível para usuários legítimos. A Figura 19 representa a árvore de ataque correspondente a esta ameaça:

Figura 19 – Árvore de ataque para ameaça de negação de serviço

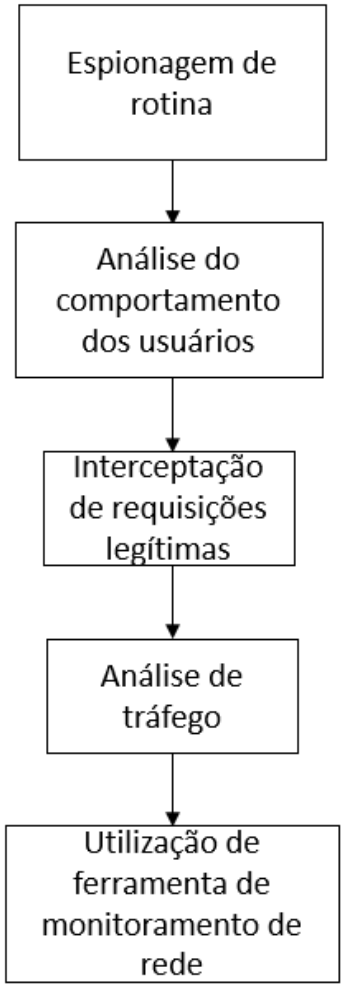


Fonte: Produzido pelo autor

Comprometendo princípios de privacidade, um atacante poderia atacar o sistema com o intuito de obter informações sobre a rotina dos residentes, as quais poderiam servir de insumo para cenários de ameaça posteriores como roubo residencial, sequestro, danos à saúde e danos financeiros. Para isto, o atacante poderia se utilizar de ferramentas de monitoramento de rede, com a intenção de interceptar o tráfego de rede entre o cliente e o servidor web.

A Figura 20 exemplifica a árvore de ataques em questão:

Figura 20 – Árvore de ataque para ameaça de espionagem de rotina



Fonte: Produzido pelo autor

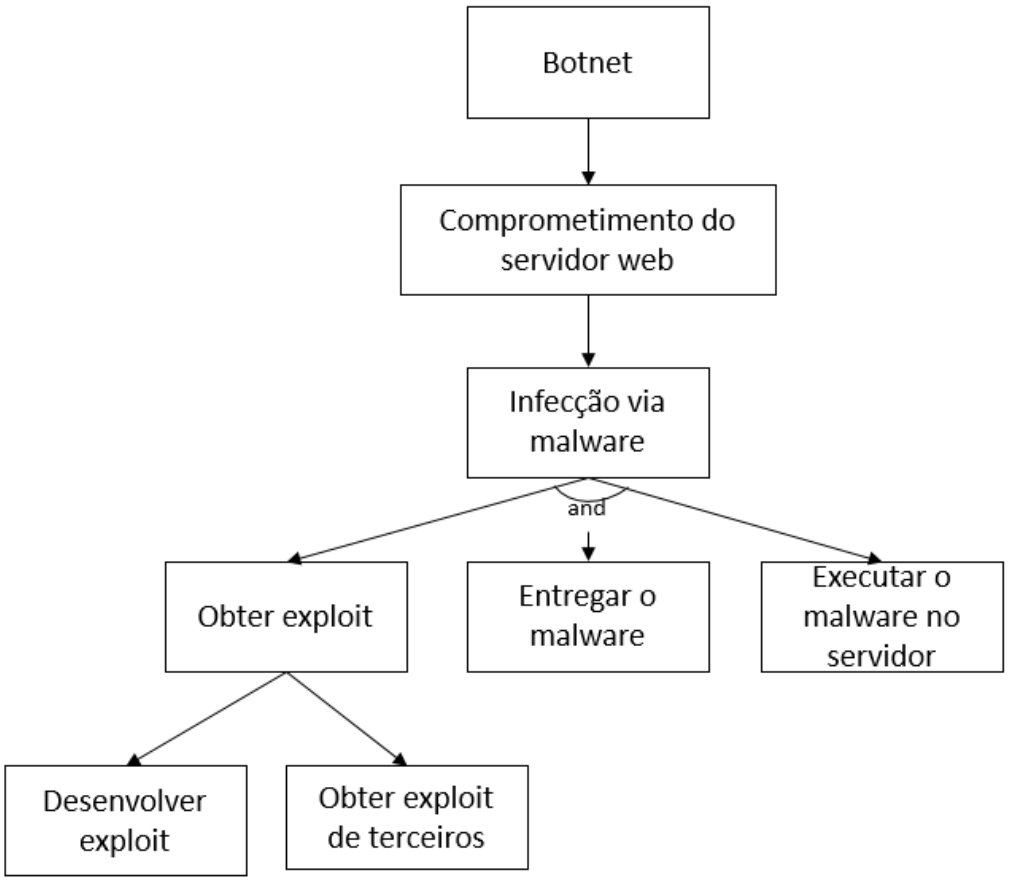
Com isto, a partir da análise do tráfego de rede interceptado, um atacante poderia inferir informações sobre a rotinas dos usuários. Por exemplo, identificar os principais horários de interação com o sistema para inferir quando usuários estariam na residência ou não. Com estas informações, um atacante elaborar ataques mais sofisticados, resultando em cenários de ameaças como os descritos nas seções anteriores.

Por último, dentre as principais ameaças e ataques envolvendo sistemas IoT, encontram-se os que visam comprometer o sistema e torna-lo parte de uma *botnet*. A ideia geral é o comprometimento do dispositivo IoT por algum *malware* que permite o controle do dispositivo IoT por um atacante, fazendo este dispositivo parte de um conjunto de dispositivos comprometidos sob seu controle.

A partir da obtenção do controle do dispositivo, um atacante poderia utilizar seu recurso computacional para, por exemplo, o processamento de informações de

seu interesse, para a execução de ações maliciosas dentro do próprio sistema IoT em questão, ou para realização de ataques em sistema externos, como em caso de um ataque de *Distributed Denial of Service* (DDoS). A árvore de ataque para este cenário é mostrada na Figura 21 :

Figura 21 – Árvore de ataque para ameaça *botnet*



Fonte: Produzido pelo autor

Para tornar o sistema parte de uma *botnet*, um atacante pode, por exemplo, infectá-lo através de um *malware.* Para isto, ele necessita obter o *malware,* realizar a entregar deste *malware* ao ativo e executar o *malware.*

5.2.3.2 Identificação de Vulnerabilidades

Utilizando as árvores de ataque como insumo, as seguintes vulnerabilidades foram identificadas para cada ameaça:

Tabela 5 – Vulnerabilidades identificadas

Ameaça	Vulnerabilidade
Danos financeiros	Fluxo de comunicação realizado sem mecanismos de criptografia e ausência de mecanismo de autenticação entre o cliente e o servidor aos serviços da API
Danos a saúde	Fluxo de comunicação realizado sem mecanismos de criptografia e ausência de mecanismo de autenticação entre o cliente e o servidor aos serviços da API
Sequestro de usuários	Fluxo de comunicação realizado sem mecanismos de criptografia e ausência de mecanismo de autenticação entre o cliente e o servidor aos serviços da API
Roubo Residencial	Fluxo de comunicação realizado sem mecanismos de criptografia e ausência de mecanismo de autenticação entre o cliente e o servidor aos serviços da API
Negação de serviço	Ausência de mecanismos de identificação e recuperação de ataques de negação de serviço.
Espionagem de rotina	Fluxo de comunicação realizado sem mecanismos de criptografia. Ou seja, em texto plano.
Botnet	Ausência de mecanismos de autenticação entre cliente e servidor e utilização de versões desatualizadas de software.

Fonte: Produzido pelo autor

Assim, percebe-se que a maioria dos cenários de ameaça são viabilizados pelo fato do sistema não utilizar mecanismos de criptografia para a realização da comunicação entre o servidor *Web* e o cliente, representado pelo aplicativo móvel. Ou seja, todo o fluxo de informações entre as principais entidades do sistema é realizado em texto plano, em um ambiente virtual inseguro, como a Internet.

Adicionalmente, o sistema não implementa nenhum mecanismo de autenticação (como login e senha) para tentar garantir a identidade de um suposto usuário. Com isto, apenas com o conhecimento do endereço IP do servidor, assim como da porta no qual o serviço está em execução, é possível que qualquer usuário (malicioso ou não) execute atividades que refletem diretamente no estado do sistema e podem levar aos cenários de ameaça citados anteriormente. Por fim, a utilização de softwares desatualizados pode levar ao comprometimento do ambiente IoT analisado.

5.2.4 Classificação de Ameaças

Após a identificação das ameaças, dos vetores de ataque que as viabilizam e da identificação de vulnerabilidades que estão associadas a cada ameaça, a classificação das ameaças de segurança foi realizada a partir dos critérios definidos no esquema de classificação proposto neste trabalho. Com isto, a seguir serão apresentadas as informações sobre o método de classificação escolhido, a aplicação do esquema de classificação e a organização das ameaças de segurança por sua respectiva severidade.

5.2.4.1 Escolha do Método de Classificação

O método de classificação escolhido para classificar as ameaças de segurança identificadas foi o método proposto neste trabalho, o qual está descrito e pode ser consultado na seção 4.6.1.

5.2.4.2 Aplicação do método de classificação

Nesta atividade, o método de classificação foi aplicado a cada ameaça de segurança mapeada na etapa de identificação. A seguir, será apresentado o resultado da aplicação do método de classificação para cada ameaça, incluindo os valores de cada propriedade, a justificativa para escolha da valoração e o valor do risco final.

- Classificação da ameaça de danos financeiros:

Tabela 6 – *Classificação da ameaça de danos financeiros*

Propriedade	*Valor*	*Justificativa*
Damage	*3*	*A ausência de mecanismos de autenticação e a realização de comunicação em texto plano entre cliente e servidor, aumentam as probabilidades de sucesso dos ataques envolvidos com esta ameaça. Uma vez que o atacante consigo comprometer servidor web, ele pode, então, controlar todos os dispositivos que compõem o sistema IoT.*

Propriedade	*Valor*	*Justificativa*
Reproducibility	*3*	*Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento.*
Exploitability	1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o cliente e o servidor e realizar ataques de repetição ou de envio de requisições maliciosamente criadas. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	3	Uma vez que um atacante comprometa o servidor web, ele consegue executar ações maliciosas que atingem e afetam todos os outros dispositivos contidos no sistema IoT.
Affected users	0	Esta ameaça não inflige risco de vida aos usuários do sistema
Discoverability	3	A descrição detalhada do sistema, assim como suas funcionalidades e tecnologias são acessíveis através de artigos publicados e facilmente acessíveis a um atacante.
Risco	2.16	

Fonte: Produzido pelo autor

- Classificação da ameaça de danos à saúde:

Tabela 7 – Classificação da ameaça de danos à saúde

Propriedade	Valor	Justificativa
Damage	3	A ausência de mecanismos de autenticação e a realização de comunicação em texto plano entre cliente e servidor, aumentam as probabilidades de sucesso dos ataques envolvidos com esta ameaça. Uma vez que o atacante consiga comprometer servidor web, ele pode, então, controlar todos os dispositivos que compõem o sistema IoT.

Propriedade	Valor	Justificativa
Reproducibility	3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento
Exploitability	1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o cliente e o servido e realizar ataques que envolvam o envio de requisições maliciosamente criadas. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected Things	3	Uma vez que um atacante comprometa o servidor web, ele consegue executar ações maliciosas que atingem e afetam todos os outros dispositivos.
Affected users	2	Embora todos os residentes possam sentir os efeitos dos ataques realizados para a realização desta ameaça, nem todos os usuários podem ter a mesma probabilidade de desencadear complicações de saúde devido as variações de temperatura umidade.
Discoverability	3	A descrição detalhada do sistema, assim como suas funcionalidades e tecnologias são acessíveis através de artigos publicados e facilmente acessíveis a um atacante.
Risco	2.5	

Fonte: Produzido pelo autor

- Classificação da ameaça de sequestro de usuários:

Tabela 8 – Classificação da ameaça de sequestro de usuários

Propriedade	Valor	Justificativa

Propriedade	Valor	Justificativa
Damage	3	A ausência de mecanismos de autenticação e a realização de comunicação em texto plano entre cliente e servidor, aumentam as probabilidades de sucesso dos ataques envolvidos com esta ameaça. Uma vez que o atacante consiga comprometer o servidor web, ele pode, então, controlar todos os dispositivos que compõem o sistema IoT.
Reproducibility	3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento
Exploitability	1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita ter acesso a residência dos usuários do sistema. Para isso, ele precisa interceptar e analisar o tráfego de comunicação entre o cliente e o servidor e realizar o envio de requisições maliciosamente criadas. Além disso, um atacante necessita realizar a análise comportamental da rotina dos usuários para uma maior efetividade de suas ações. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	3	Uma vez que um atacante comprometa o servidor web, ele consegue executar ações maliciosas que atingem e afetam todos os outros dispositivos.
Affected users	3	Risco direto à vida dos usuários.
Discoverability	3	A descrição detalhada do sistema, assim como suas funcionalidades e tecnologias são acessíveis através de artigos publicados e facilmente acessíveis a um atacante.
Risco	2.66	

Fonte: Produzido pelo autor

- Classificação da ameaça de negação de serviço:

Tabela 9 – Classificação da ameaça de negação de serviço

Propriedade	Valor	Justificativa
Damage	3	Uma vez que o atacante torne o servidor indisponível, todos os serviços de gerenciamento remoto através da API também estarão. Com isto, todos os dispositivos do sistema são afetados.
Reproducibility	3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento
Exploitability	3	Ferramentas de geração de automática de tráfego são facilmente acessíveis e não requerem um alto nível técnico para a realização do ataque envolvido.
Affected things	3	Ao tornar o servidor web indisponível, todas os dispositivos que compõem o sistema também estarão.
Affected users	0	Esta ameaça não inflige risco de vida aos usuários do sistema
Discoverability	3	A descrição detalhada do sistema, assim como suas funcionalidades e tecnologias são acessíveis através de artigos publicados e facilmente acessíveis a um atacante
Risco	2.5	

Fonte: Produzido pelo autor

- Classificação da ameaça de espionagem de rotina:

Tabela 10 – Classificação da ameaça de espionagem de rotina

Propriedade	Valor	Justificativa
Damage	2	Para este cenário de ameaça, um atacante visaria apenas a interceptação do tráfego entre o cliente e o servidor web, não visando o comprometimento direto do ativo.
Reproducibility	3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento.
Exploitability	1	Ferramentas de monitoramento de tráfego de rede são amplamente acessíveis e possuem tutoriais disponíveis na web. Contudo, se faz necessário um conhecimento técnico aprofundado para que um atacante identifique o tráfego correto e possa obter sucesso na análise de rotina dos residentes.
Affected things	2	O ataque visa comprometer apenas a confidencialidade da comunicação entre o cliente e o servidor.
Affected users	0	Embora a ameaça fira princípios de privacidade dos usuários, este não afeta os usuários de forma a pôr a vida destes em risco.
Discoverability	3	A descrição detalhada do sistema, assim como suas funcionalidades e tecnologias são acessíveis através de artigos publicados e facilmente acessíveis a um atacante.
Risco	1.83	

Fonte: Produzido pelo autor

- Classificação da ameaça botnet:

Tabela 11 – Classificação da ameaça *botnet*

Propriedade	Valor	Justificativa
Damage	3	Uma vez que o atacante consiga comprometer o servidor web, ele pode controlar este dispositivo e executar comandos como um administrador.
Reproducibility	1	O conjunto de ataques, assim como a complexidade destes, tornam esta ameaça de difícil reprodução.

Propriedade	Valor	Justificativa
Exploitability	1	Para que um atacante comprometa o sistema se faz necessário o conhecimento das tecnologias que o compõe, das vulnerabilidades associadas, da disponibilidade/criação de exploits e a realização da entrega e execução do exploit pelo dispositivo alvo. Este conjunto de fatores requer um atacante com uma alta expertise técnica.
Affected things	3	Uma vez que um atacante comprometa o servidor web, ele consegue executar ações maliciosas que atingem e afetam todos os outros dispositivos.
Affected users	0	Embora o atacante possa escalar para ataques que visem danos aos usuários do sistema, o intuito principal deste tipo de ameaça é o ganho pessoal de um atacante.
Discoverability	1	Embora haja uma descrição detalhada e pública do sistema, apenas um atacante com um alto conhecimento técnico teria condições de enxergar os vetores de ataque que envolvem esta ameaça.
Risco	1.5	

Fonte: Produzido pelo autor

5.2.4.3 Organização de Ameaças por Severidade

Após a classificação das ameaças e a atribuição dos seus devidos riscos, as ameaças foram organização pelo respectivo valor de seu risco. O ranking das ameaças baseado em seus riscos é mostrado na Tabela :

Tabela 12 – Ranking de ameaças

Ameaça	Risco
Sequestro de usuários	2.66
Roubo residencial	2.5
Danos à saúde	2.5
Negação de serviço	2.5
Danos financeiros	2.16
Espionagem de rotina	1.83
Botnet	1.5

Fonte: Produzido pelo autor

A organização das ameaças de acordo com o seu risco associado permite a priorização dos esforços de segurança no que se refere a implantação de contramedidas e consequente mitigação dessas ameaças.

5.2.5 Documentação de Artefatos

A etapa de documentação visa formatar os artefatos gerados durante a aplicação da metodologia. O documento gerado a partir do agrupamento e documentação dos artefatos produzidos pela modelagem de ameaças tem por objetivo gerar um modelo de ameaças.

Como explanado na seção 4.7, um modelo de ameaças é um documento que é composto pelos seguintes artefatos: diagrama arquitetural de fluxo de dados (Figura 13), ameaças de segurança identificadas (apresentadas na seção 5.2.2), árvores de ataque (seção 5.2.3.1), vulnerabilidades (seção 5.2.3.2), classificação das ameaças (seção 5.2.4.2) e *ranking* de ameaças (seção 5.2.4.3). Com isto, tais artefatos podem ser organizados e documentados de forma a serem apresentados conforme a preferência de formatação de seus usuários.

Como a documentação da aplicação deste estudo de caso através desta monografia contempla a inclusão de tais artefatos, estes não serão reapresentados nesta seção por questões de redundância.

5.3 Resultados e Discussão

Esta seção visa ressaltar os principais resultados obtidos com a aplicação da metodologia proposta neste trabalho ao ambiente analisado no estudo de caso. É importante destacar que, no geral, o processo de modelagem de ameaças visa identificar, categorizar e classificar as ameaças de segurança de um objeto de análise. Através da aplicação desta metodologia ao cenário estudado, buscou-se, principalmente, verificar a sua adequabilidade ao contexto da Internet das Coisas, de forma a ser aplicável em contextos diversos de IoT, considerando as propriedades inerentes a este paradigma.

Em termos de identificação de ameaças, foi possível identificar um conjunto de ameaças de segurança diretamente ligadas ao cenário de estudo, considerando as características do cenário IoT analisado. Também se verificou que as ameaças e ataques retratados nos cenários de ameaça se adequavam em uma ou mais categorias definidas no método de categorização proposto nesta pesquisa. Isto demonstra que, a utilização das atividades propostas por esta metodologia conduziu ao objetivo esperado para a etapa de identificação de ameaças, viabilizando insumos para as demais etapas

do processo.

O esquema de categorização proposto na seção 4.4 apresenta uma cobertura dos principais ataques realizados contra o ambiente e os organiza por categorias. Como levantado na seção de justificativa, os métodos de categorização propostos pelas metodologias generalistas poderiam não incluir categorias de ameaças características da Internet das Coisas. Tal suposição se mostrou verdadeira pois, através do estudo e proposição do método de categorização deste trabalho, percebeu-se padrões de ataques que diferem dos contextos generalistas e que, provavelmente, não seriam cobertos pelas categorias de ameaças proposta por estes.

A classificação de ameaças de ameaças de segurança também demonstrou concisão em seus resultados. Ao observar a Tabela 11, responsável por representar o *ranking* de classificação de ameaças baseada em seus riscos, é possível notar a coesão de criticidade das ameaças identificadas. Observa-se, por exemplo, que a ameaça mais crítica (sequestro de usuários) é representada pelo cenário que viabilizaria um maior risco à vida dos usuários do sistema. Também, é válido notar que a ameaça apontada como menos crítica (*botnet*) é a que possui menor viabilidade de concretização e promove o menor risco à vida dos usuários do sistema IoT. Tais resultados apontam evidências inicias que o método de classificação proposto neste trabalho é interessante. Além desta coerência lógica, é possível perceber a relevância da inclusão e ajuste das propriedades adicionadas como extensão do método de classificação proposto, tendo por base o método apresentado em Sándor e Sebestyén-Pál (2017).

Em suma, este estudo de caso demonstra que a metodologia proposta cumpre com seus objetivos. Ou seja, apresenta sucesso ao identificar, categorizar e classificar as ameaças de segurança em um ambiente baseado na Internet das Coisas, levando em consideração as propriedades e características do paradigma.

6 Conclusão

6.1 Conclusões

O rápido crescimento e expansão da Internet das Coisas tem permitido aplicações que objetivam tornar a vida cotidiana mais prática, produtiva, confortável e segura. Contudo, devido à alta heterogeneidade das tecnologias que compõem a Internet das Coisas, aumenta-se a superfície de ataque e, consequentemente, os riscos de segurança associadas a estes ambientes. Com isto, faz-se necessário a proposição de técnicas, métodos e soluções que visem tratar das questões de segurança em IoT.

Neste sentido, este trabalho apresentou uma metodologia de modelagem de ameaças de segurança aplicável a ambientes baseados na Internet das Coisas. Para isto, este trabalho analisou os principais referenciais teóricos, buscando identificar e analisar as principais metodologias vigentes e propostas para cenários generalistas (os quais não são focados em IoT) e trabalhos que realizavam propostas inicias de modelagem de ameaças na Internet das Coisas. A partir do referencial teórico, foi possível definir uma metodologia base, a qual foi refinada através do estudo de suas propriedades em contraste com sua adequação ao contexto de IoT. Ao fim deste processo, este trabalho foi capaz de propor uma metodologia aplicável a Internet das Coisas, considerando as propriedades necessárias para a identificação, categorização e classificação de ameaças em IoT.

Através do desenvolvimento e aplicação da metodologia proposta neste trabalho, foi possível observar o sucesso na identificação e classificação de ameaças de segurança em IoT, considerando as propriedades inerentes a este paradigma. Para isto, este trabalho também propôs um esquema de classificação de ameaças baseado nos principais ataques direcionados à Internet das Coisas, identificados em trabalhos existentes na literatura. No que concerne à classificação de ameaças, este trabalho também apresenta um método de classificação de ameaças, baseado na extensão do método de classificação proposto por Sándor e Sebestyén-Pál (2017), adicionando propriedades de classificação que levam em consideração o risco direto à vida dos usuários frente à ameaça analisada.

Em suma, este trabalho se mostrou bem sucedido ao atender o objetivo geral e questão de pesquisa, os quais guiaram o desenvolvimento desta pesquisa. Através do estudo de caso realizado, foi possível utilizar a metodologia proposta, evidenciando a utilidade desta metodologia no processo de modelagem de ameaças em IoT. Como as principais contribuições para o meio científico e acadêmico, pode-se citar a proposição da própria metodologia de modelagem de ameaças de segurança aplicável a ambientes

IoT a qual pode servir de referência para a evolução e refinamento desta técnica por outros pesquisadores. Adicionalmente, embora ainda necessite de melhorias, pode-se também destacar a proposta de um esquema categorização inicial das ameaças de segurança na Internet das Coisas e um método de classificação adaptado as características inerentes às ameaças associadas a sistemas IoT.

Com isto, espera-se que este trabalho migre os principais benefícios já apresentados pelas metodologias generalistas para o âmbito de segurança na Internet das coisas, os quais já foram apresentados em seções anteriores e podemos destacar: método sistemático para identificação, categorização e classificação de ameaças em IoT, o auxílio na identificação mais efetiva de contramedidas de segurança baseada nas ameaças identificadas, insumos concretos para justificar os esforços de segurança e a extração de requisitos de segurança.

6.2 Trabalhos Futuros

Como trabalhos futuros, espera-se aplicar a metodologia desenvolvida em ambientes IoT mais diversificados. Neste trabalho, foi possível aplicar a metodologia proposta em um ambiente analisado. O ambiente no qual o estudo de caso foi realizado compreendeu o domínio de casas e ambientes inteligentes. Com isto, espera-se aplicar a metodologia em ambientes que compreendam outros domínios, como *healthcare*, carros inteligentes, aplicações pessoais e sociais, e verificar sua aplicabilidade de forma mais ampla.

Também propõe-se avaliar o produto deste trabalho a partir da sua utilização por um grupo de usuários observados. Tais usuários podem ser, por exemplo, profissionais da área de segurança da informação que se disponibilizem a utilizar e avaliar esta metodologia. Desta forma, espera-se obter insumos que auxiliem no processo de refinamento da metodologia em termos de usabilidade, compreensão e melhoria de aspectos técnicos, através de fontes de avaliação diversificadas.

Devido à alta heterogeneidade inerente à Internet das Coisas, um estudo mais aprofundado é necessário para mapear de forma mais abrangente os tipos de ameaças e ataques aos quais os ambientes IoT estão potencialmente expostos e, consequentemente atualizar as categorias de ataques correspondentes. Além disso, faz-se necessário um estudo mais aprofundado sobre as propriedades utilizadas para a classificação de ameaças com o intuito de aperfeiçoar as métricas usadas para classificar o risco das ameaças de segurança identificadas.

Referências

ABOMHARA, M.; KØIEN, G. M. Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, p. 1 – 8, 2014.

ATAMLI, A. W.; MARTIN, A. Threat-Based Security Analysis for the Internet of Things. *2014 International Workshop on Secure Internet of Things, Wroclaw, 2014,*, p. 35 – 43, 2014.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. *Computer Networks*, v. 54, p. 2787 – 2805, 2010.

CHOWDHURY, N. M.; MACKENZIE, L. Development of a Threat Model for Vehicular Ad-hoc Network based Accident Warning Systems. *Proceedings of the 7th International Conference on Security of Information and Networks*, p. 1 – 12, 2014.

COVINGTON, M. J.; CARSKADDEN, R. Threat implications of the Internet of Things. *2016 3rd International Conference on Electronic Design (ICED)*, p. 321 – 326, 2016.

DEOGIRIKAR, J.; VIDHATE, A. Security attacks in IoT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, p. 32 – 37, 2017.

DUNCAN, A. B.; FELLOUS, S.; KALTZ, O. *Temporal variation in temperature determines disease spread and maintenance in Paramecium microcosm populations*. 2013. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3177632/>. Acesso em: 15/01/2018.

EUROPEAN RESEARH CLUSTER ON INTERNET OF THINGS. *IoT Governance, Privacy and Security*. 2015. Disponível em: <http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf>. Acesso em: 29/06/2017.

GARTNER. *Gartner says the Internet of Things installed base will grow to 26 billion units by 2020*. 2013. Disponível em: <http://www.gartner.com/newsroom/id/2636073>. Acesso em: 23/06/2017.

GUBBI et al. Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems. *Future Generation Computer Systems*, v. 29, p. 1645 – 1660, 2013.

IRSHAD, M. A Systematic Review of Information Security Frameworks in the Internet of Things (IoT). *2016 IEEE 18th International Conference on High Performance Computing and Communications*, p. 1270 – 1275, 2016.

JADOUL. *The next step in internet evolution*. 2015. Disponível em: <https://insight.nokia.com/iot-next-step-internet-evolution>. Acesso em: 29/06/2017.

KRAIJAK, S.; TUWANUT, P. A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, p. 26 – 31, 2015.

MICROSOFT. *Threat Modeling*. 2003. Disponível em: <https://msdn.microsoft.com/en-us/library/ff648644.aspx>. Acesso em: 16/06/2017.

MICROSOFT. *Threat Modeling Tool*. 2016. Disponível em: <https://www.microsoft.com/en-us/download/details.aspx%3Fid%3D49168>. Acesso em: 10/01/2018.

NAWIR, M.; AMIR, A.; YAAKOB, N. Internet of Things (IoT): Taxonomy of security attacks. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, p. 1 – 12, 2013.

OBJECT MANAGEMENT GROUP. Business Process Model and Notation. 2011.

OWASP. *Threat Risk Modeling*. 2006. Disponível em: <https://www.owasp.org/index.php/Threat_Risk_Modeling>. Acesso em: 18/06/2017.

PIYARE, R. Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone. *International Journal of Internet of Things 2013*, p. 5 – 11, 2013.

REIS, H. T. E. dos. Segurança da informação e a Educação a distância. *Oficina de Lingua Portuguesa – Literatura e Produção de Texto*, p. 1 – 10, 2011.

SAIN, M.; KANG, Y. J.; LEE, H. J. Survey on security in Internet of Things: State of the art and challenges. *19th International Conference on Advanced Communication Technology*, p. 699 – 704, 2017.

SAITTA, P.; LARCOM, B.; EDDINGTON, M. *Trike v.1 Methodology Document [Draft]*. 2005. Disponível em: <http://octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf>. Acesso em: 23/07/2017.

SÁNDOR, H.; SEBESTYÉN-PÁL, G. Optimal security design in the Internet of Things. *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, p. 1 – 6, 2017.

WANG, P.; ALI, A.; KELLY, W. Data security and threat modeling for smart city infrastructure. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, p. 1 – 6, 2015.

ZHANG, Z. et al. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, p. 230 – 234, 2014.