
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
Curso Superior de Tecnologia em Segurança da Informação

Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios

Leandro Rogério Corrêa Leite

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
Curso Superior de Tecnologia em Segurança da Informação

Internet das Coisas (IoT): Vulnerabilidades de Segurança e Desafios

Leandro Rogério Corrêa Leite

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Ms. Rogério Nunes de Freitas.

Área de concentração: Segurança da Informação em Internet das Coisa

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

L554i LEITE, Leandro Rogério Corrêa

Internet das coisas (IoT): vulnerabilidades de segurança e desafios. / Leandro Rogério Corrêa Leite. – Americana, 2019.

80f.

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

Orientador: Prof. Ms. Rogério Nunes de Freitas

1 Internet das coisas I. FREITAS, Rogério Nunes de II. Centro Estadual de
Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518

Faculdade de Tecnologia de Americana

Leandro Rogério Corrêa Leite


Internet das Coisas (IoT)
Vulnerabilidades de Segurança e Desafios

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.

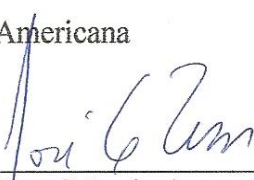
Área de concentração: Segurança da Informação em Internet das Coisa

Americana, 04 de Dezembro de 2019.

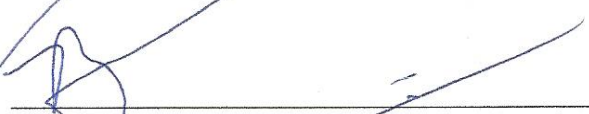
Banca Examinadora



Rogério Nunes de Freitas (Presidente)
Mestre
FATEC – Americana



José Luis Zem (Membro)
Doutor
FATEC – Americana



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

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade em chegar até aqui e estar concluindo mais um ciclo em minha vida.

À minha esposa e aos meus pais pelos inúmeros incentivos e por consentir em abrir mão da parcela de tempo dedicada à minha formação.

Ao professor Ms. Rogério Nunes de Freitas pela grande competência em sua orientação e por mostrar o caminho a ser trilhado, compartilhando seu vasto conhecimento.

À Professora Dra. Maria Cristina Aranda Batocchio que foi essencial na elaboração desta monografia, através de seu conhecimento, paciência e grande incentivo

Agradeço a todos os professores, amigos e colegas, que direta ou indiretamente contribuíram na elaboração deste projeto.

DEDICATÓRIA

Dedico este trabalho a minha família, que sempre esteve presente em todos os momentos da minha vida, em especial a minha esposa Rosilene e minha filha Alice.

RESUMO

A Internet das Coisas ou IoT (Internet of Things) é uma tecnologia que vem crescendo muito e ganhando destaque no cenário mundial. Com o objetivo de interligar objetos e equipamentos que são utilizados no cotidiano; esta tecnologia promete trazer inúmeros benefícios tanto para o uso doméstico como industrial. Porém existem alguns obstáculos que devem ser levados em consideração, principalmente quando o assunto é a segurança das informações que estão nestes dispositivos. O presente trabalho aborda os problemas referentes à segurança da informação envolvendo a tecnologia IoT, apontando os riscos, vulnerabilidades e ameaças que a adoção desta tecnologia pode trazer e também apresenta um conjunto de possíveis soluções que podem ser adotadas para mitigar os problemas encontrados neste tipo de ambiente. O trabalho está dividido em sete capítulos. No capítulo um é apresentado uma introdução ao tema da pesquisa e logo no capítulo dois são abordados os conceitos de redes de computadores e Internet. No capítulo três são abordados os conceitos de segurança da informação apresentando os três pilares básicos. No capítulo quatro é apresentada a tecnologia IoT, desde seu surgimento, evolução, benefícios até os principais desafios encontrados. No capítulo cinco são abordados, com maiores detalhes, as questões de segurança relacionadas à tecnologia IoT, bem como as vulnerabilidades, tipos de ataques e principais métodos de segurança. No capítulo seis é apresentado um guia de boas práticas juntamente com recomendações de especialistas da área de Segurança da Informação, baseadas em artigos acadêmicos e publicações técnicas. Por fim, no capítulo sete, são abordadas algumas considerações finais sobre o trabalho.

Palavras Chaves: Ataques; Internet das Coisas; Segurança; Vulnerabilidades.

ABSTRACT

The Internet of Things (IoT) is a technology that has been increasing a lot and has been gaining prominence in the world. This technology aims to interconnect objects and equipment that are used in everyday life and promises many benefits for both domestic and industrial use. But there are some issues that should be considered, especially when it comes to the security of the information that is present on these devices. This research addresses the problems related to information security involving the IoT technology, pointing out the risks, vulnerabilities and threats that the adoption of this technology can bring and features a set of possible solutions that can be taken to mitigate the problems encountered in this type of environment. This research is divided into seven chapters. In the chapter one, is approach an introduction to the research theme and in the chapter two are presented the concepts of computer networking and the Internet. In the chapter three is approach the concept of Security Information by presenting the three basic pillars. In the chapter four, the IoT technology is presented, since its emergence, evolution, benefits and main challenges. In the chapter five, IoT-related security issues are covered in more detail, presenting vulnerabilities, types of attacks, and key security methods. In the chapter six is presents a good practice guide supported by recommendations from Information Security experts based on scholarly articles and technical publications. Finally, in the chapter seven, is approach some final considerations about the research.

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

SUMARIO

INTRODUÇÃO	15
1. REDES DE COMPUTADORES E INTERNET	17
1.1 A Evolução da Web e da Internet	18
2. SEGURANÇA DA INFORMAÇÃO.....	20
2.1 Os Três Pilares da Segurança da Informação	21
3. A Internet das Coisas	23
3.1 Dispositivos e Tecnologia de Comunicação.....	25
3.2 Benefícios da Tecnologia IoT.....	26
3.3 Principais Desafios	29
3.3.1 Armazenamento	29
3.3.2 Conectividade.....	29
3.3.3 Energia	29
3.3.4 Padronização	30
3.3.5 Segurança / Privacidade	30
4. SEGURANÇA DA INFORMAÇÃO NA IoT.....	32
4.1 Vulnerabilidades Possíveis em Ambientes IoT	33
4.1.1 Senhas fracas, previsíveis ou dentro do código	34
4.1.2 Serviços de rede inseguros	34
4.1.3 Ecossistema de interfaces inseguros	35
4.1.4 Falta de mecanismos de atualização seguros.....	35
4.1.5 Uso de componentes inseguros ou obsoletos	35
4.1.6 Proteção da privacidade insuficiente	35
4.1.7 Transferência e armazenamento de dados de maneira insegura	35
4.1.8 Falta de controle de gerenciamento dos dispositivos	36
4.1.9 Configuração insegura por padrão	36
4.1.10 Segurança física insuficiente	36
4.2 Ataques Possíveis em Ambientes IoT	37
4.2.1 Ataques Físicos	37
4.2.2 Ataques de Rede.....	39
4.2.3 Ataques de Software	41
4.2.4 Ataques de Criptografia.....	41
4.3 Principais Métodos de Segurança para IoT	44
5. BOAS PRÁTICAS NA IMPLEMENTAÇÃO DA IOT	47
5.1 Casos de Invasões Documentados	47
5.1.1 Lâmpadas inteligentes podem estar vulneráveis a ataques de hackers.....	47
5.1.2 Falhas permitem acesso de hackers a câmeras inteligentes	49
5.1.3 Maior ataque DDoS da história foi causado por botnet de dispositivos IoT sequestrados.....	50
5.2 Guia para o Desenvolvimento de Dispositivos IoT Seguros	51
5.2.1 Iniciar com uma metodologia de desenvolvimento seguro	52
5.2.2 Implementar um ambiente seguro de desenvolvimento e integração	54

5.2.3 Identificar recursos de segurança da estrutura e da plataforma.....	56
5.2.4 Estabelecer proteções de privacidade.....	58
5.2.5 Projetar controles de segurança em hardware	59
5.2.6 Fornecer proteção dos dados.....	61
5.2.7 Garantir o desenvolvimento de aplicativos e serviços seguros	64
5.2.8 Proteger interfaces / APIs.....	65
5.2.9 Fornecer recursos de atualizações de segurança.....	66
5.2.10 Implementar recursos de autenticação e controle de acesso.....	67
5.2.11 Estabelecer recursos de gerenciamento de chaves de segurança	70
5.2.12 Fornecer mecanismos de registros	72
5.2.13 Executar análises de segurança	72
CONSIDERAÇÕES FINAIS.....	74
REFERÊNCIAS	76

LISTA DE ABREVIATURA E SIGLAS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ABNT	Associação Brasileira de Normas Técnicas
AC	Alternating Current
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
API	Application Programming Interface
Arpanet	Advanced Research Projects Agency Network
Bitnet	Because It's Time to Network
BSIMM	Building Security In Maturity Model
CA	Certificate Authority
CC	Common Criteria
CDMA	Code Division Multiple Access
CLAE	Certificate-Less Authenticated Encryption
CoAP	Constrained Application Protocol
CPS	Cyber Physical Systems
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CSnet	Computer Science Network
DAST	Dynamic Application Security Testing
DC	Direct Current
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
Decnet	Digital Equipment Corporation Network
DoD	Department of Defense
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
Earn	European Academic & Research Network
ECDH	Elliptic Curve Diffie Hellman
EST	Enrollment over Secure Transport
EUA	Estados Unidos da America
Fidonet	Fido Network
Gbps	Gigabits por Segundo

GEA	GPRS Encryption Algorithm
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
Hepnet	High-Energy Physics Network
HTTP	Hypertext Transfer Protocol
IAST	Interactive Application Security Testing
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
Janet	Joint Information Systems Committee Network
JTAG	Joint Test Action Group
Junet	Japan University NETwork
LoRaWAN	Long Range Wide Area Network
LoWPAN	Low Power Wireless Personal Area Networks
LTE	Long Term Evolution
M2M	Machine-to-Machine
MHz	Megahertz
MISRA	Motor Industry Software Reliability Association
MIT	Massachusetts Institute of Technology
MITM	Man in The Middle
MPU	Memory Protection Unit
MQTT	Message Queuing Telemetry Transport
NBR	Norma Técnica Brasileira
Netnorth	North America Network
NFC	Near Field Communication
NS	Nó Sensor
NSF	National Science Foundation
NSFnet	National Science Foundation Network
OWASP	Open Web Application Security Project
P&G	Procter & Gamble
PAKE	Password Authenticated Key Exchange
PHY	Physical Layer

REST	Representational State Transfer
RFID	Radio-Frequency IDentification
RSSF	Redes de Sensores Sem Fio
SASL	Simple Authentication and Security Layer
SAST	Static Application Security Testing
SCEP	Simple Certificate Enrollment Protocol
SIM	Subscriber Identity Module
SoC	System On Chip
SSDL	Secondary Standards Dosimetry Laboratories
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TI	Tecnologia da Informação
TLS	Transport Layer Security
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UMA	User Managed Access
UMTS	Universal Mobile Telecommunication System
UNB	Ultra Narrow Band
USB	Universal Serial Bus
Vnet	Virtual Network
XMPP	Extensible Messaging and Presence Protocol
ZAP	Zed Attack Proxy

LISTA DE FIGURAS

Figura 1 - Estrutura Básica de uma Rede de Computadores	17
Figura 2 - Pilares da Segurança da Informação	21
Figura 3 - A Evolução da IoT	23
Figura 4 - Interações na IoT	24
Figura 5 - Arquitetura dos Dispositivos IoT	25
Figura 6 - Panorama do Mercado de IoT	27
Figura 7 - Relatório Global de Riscos.....	32
Figura 8 - Lâmpada Inteligente Positivo	48
Figura 9 - Câmera Inteligente Multidirecional PNM-9084QZ	49
Figura 10 - Etapas para O Desenvolvimento Seguro da IoT	51
Figura 11 - Pirâmide de Teste de Martin Fowler	55
Figura 12 - Criptografia de Autenticação Sem Certificado	69

LISTA DE TABELAS

Tabela 1 - Classificação dos Ataques a IoT	43
Tabela 2 - Medidas de Contra-Ataque para IoT	44
Tabela 3 - Modelo de Maturidade de Desenvolvimento Seguro.....	53
Tabela 4 - Protocolos para Dispositivos IoT.....	63
Tabela 5 - Protocolos para Autenticação M2M.....	68
Tabela 6 - Processo de Geração de Chaves Criptográficas	71

INTRODUÇÃO

Atualmente a informação apresenta uma crescente importância e tem se tornado fundamental para as empresas na descoberta e introdução de novas tecnologias, exploração das oportunidades de investimento e ainda no planejamento de toda a atividade industrial.

E é por esse motivo que a Segurança da Informação tem se tornado cada vez mais importante no âmbito empresarial, a fim de proteger esse ativo valioso, crítico e sensível, sobretudo em um mundo conectado, que está presente no cotidiano das pessoas e corporações.

A IoT refere-se a uma revolução tecnológica por meio da qual objetos usados no cotidiano como eletrodomésticos, meios de transporte e até mesmo roupas estão sendo conectados à rede mundial de computadores com o intuito de interagir entre si e poder oferecer recursos e serviços mais personalizados e no momento ideal, sem a necessidade de uma programação prévia dos usuários. Para que essa nova tecnologia funcione será necessária a coleta de muitas informações das pessoas ou empresas que se proponham utilizá-la.

A justificativa na escolha do tema baseia-se no fato de que a IoT estará adicionando milhões de novos dispositivos à infraestrutura de rede global, de diferentes fabricantes e com características e configurações distintas e que justamente por estarem interconectados, apresentam vulnerabilidades que podem ser exploradas, tornando as informações alvo de ataques, pondo em risco a disponibilidade, integridade e confidencialidade das mesmas.

O objetivo geral deste estudo foi analisar os problemas relacionados à segurança da informação que podem surgir com a utilização indiscriminada da IoT. Os objetivos específicos foram: a) identificar as vulnerabilidades, ameaças e tipos de ataque em dispositivos IoT; b) expor casos notórios de problemas de segurança envolvendo IoT e, c) propor as possíveis soluções e contramedidas para os problemas encontrados e como tornar o ambiente IoT mais seguro.

O método científico utilizado nesta pesquisa foi o hipotético-dedutivo, que segundo Popper (2013), conduz o pesquisador a ser altamente cético sobre um

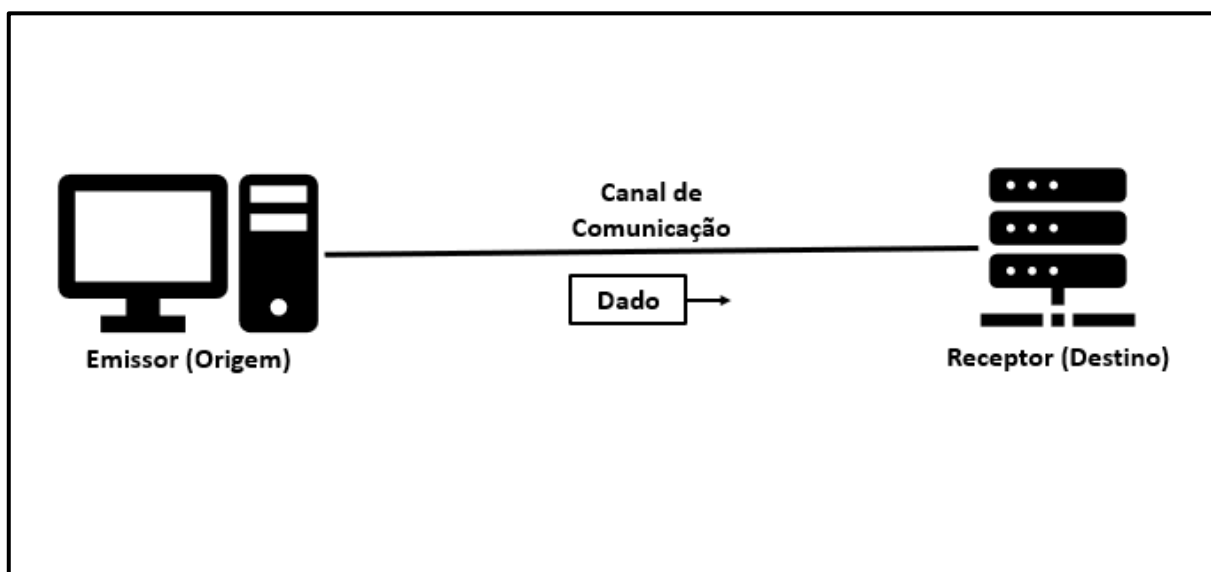
determinado assunto, buscando a remoção dos erros de uma hipótese. Partindo da ideia de que ao testar a falsidade de uma proposição, a partir de uma hipótese, estabelecendo que o fato ou resultado experimental nega essa hipótese e tentando realizar experimentos para negá-la. Assim, a abordagem do método hipotético-dedutivo é a de buscar a verdade eliminando tudo o que é falso.

1. REDES DE COMPUTADORES E INTERNET

O termo redes de computadores pode ser definido como um conjunto de computadores autônomos interconectados por uma única tecnologia com a finalidade de trocar informações (TANENBAUM, 2003). Uma rede consiste em dois ou mais dispositivos interconectados por cabo ou conexão sem fio, integrados por um sistema de comunicação e capazes de compartilharem recursos e serviços.

A estrutura de uma rede é composta basicamente por um emissor (origem), o meio pela qual a informação trafega (canal) e por fim um receptor (destino). A Figura 1 mostra a estrutura básica de uma rede de computadores:

Figura 1 - Estrutura Básica de uma Rede de Computadores



Fonte: Adaptado de Tanenbaum (2003)

Com o passar dos anos, este processo teve inúmeras melhorias de forma que a comunicação se tornou mais rápida e a conexão se tornou mais fácil e eficiente, até que se chegou a criação da Internet.

1.1 A Evolução da Web e da Internet

A Internet pode ser entendida como um conjunto de diferentes tipos de redes interconectadas através de protocolos de comunicação comuns com o objetivo de fornecerem determinados serviços (TANENBAUM, 2003) e passou por vários momentos durante seu processo evolutivo, os quais são descritos a seguir:

1º Momento: Segundo Mandel, Simon e Delyra (1997), nos anos 1960 surge a Arpanet (Advanced Research Projects Agency Network), financiada pelo Departamento de Defesa dos EUA (DoD) com o objetivo de desenvolver um sistema de comunicação descentralizado, com o intuito de não ser interrompido em caso de um possível ataque local, já que nessa época a guerra fria estava no auge. Ainda segundo os mesmos autores, a Arpanet foi um grande sucesso, porém seu acesso era restrito às instituições que possuíam contrato com o DoD. Com o aumento do interesse por este novo meio de comunicação surge então, no final dos anos 1970, a CSnet (Computer Science Network), uma rede computacional mais barata e que interligou todos os departamentos de Ciência da Computação dos EUA.

2º Momento: Nos anos 1980, surgiram várias redes, tais como Decnet, Vnet, Bitnet, Hepnet, Janet, Junet, Earn, Netnorth, Fidonet, entre outras, e a Arpanet começou a ter seu uso reduzido devido à baixa velocidade de suas linhas, que eram de 56 Kbps. Devido ao grande interesse que o meio acadêmico demonstrava na conexão à rede, em 1987, a NSF (National Science Foundation) iniciou um grande investimento no desenvolvimento de uma rede acadêmica de alta velocidade e que ampliou a conectividade entre os centros acadêmicos, surgindo então a NSFnet. Com a proliferação dessas redes os protocolos TCP/IP tornaram-se o padrão predominante e isso facilitou a interligação das redes independentes. A grande rede, resultante de todas estas redes independentes, deu origem ao que conhecemos hoje como Internet (MANDEL; SIMON; DELYRA, 1997).

3º Momento: No início dos anos 2000 ocorreu a terceira evolução da Internet que passou de um patamar estático para um ambiente dinâmico, conhecida também como web 2.0 (O'REILLY, 2005), visto que antes o foco era a entrega e consumo de conteúdo passando para a interação com os usuários. Nessa nova fase se destacam

a comercialização de produtos e serviços e empresas como o eBay e a Amazon tiveram um grande crescimento (EVANS, 2011).

4º Momento (Atual): Esta fase também é conhecida como a Web “social” ou de “experiência”, quando empresas como Google, Facebook e Twitter tornaram-se lucrativas ao conectar as pessoas ao mundo digital, permitindo o compartilhamento de informações como fotos, vídeos e textos (EVANS, 2011).

Embora a Internet tenha passado por inúmeros aperfeiçoamentos, ela prossegue realizando o mesmo que foi projetada para fazer desde a criação da Arpanet, ou seja, interligando computadores através de protocolos comuns. Segundo Evans (2011, p. 6), especialista de tecnologia futurista da empresa CISCO:

A IoT pode ser considerada como a primeira evolução real da Internet, um salto que levará a aplicações revolucionárias com potencial para melhorar consideravelmente a forma como as pessoas vivem, aprendem, trabalham e se divertem, pois ela transformou a Internet em algo sensorial (temperatura, pressão, vibração, iluminação, umidade e estresse), permitindo que sejamos mais proativos e menos reativos.

2. SEGURANÇA DA INFORMAÇÃO

O mundo moderno tem dedicado especial atenção à informação, já que esta tem se apresentado como o bem de maior valor para as organizações e também para as pessoas comuns. A boa informação abre oportunidades para quem as possui, o que torna o cenário dos negócios mais dinâmico e acirrado, em contrapartida, a ausência da informação ou a informação de má qualidade constitui uma grande ameaça, podendo levar empresas à extinção. Sendo assim podemos considerar a informação como um ativo essencial aos negócios de uma organização e que necessita ser protegida (DANTAS, 2011).

Para a devida proteção da informação, alguns conceitos devem ser compreendidos e aqui destacam-se as definições específicas para dados, informação, conhecimento e inteligência.

Os dados compreendem a classe mais baixa da informação, já a informação é composta pelos dados processados para serem utilizados de forma compreensiva, o conhecimento é a informação cuja relevância, confiabilidade e importância foram avaliadas, e a inteligência é a parte do conhecimento que habilita a tomada das melhores decisões (CARDOSO JUNIOR, 2005 *apud* DANTAS, 2011).

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Sêmola (2013) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Já na seção introdutória da norma NBR 27002:2005 (ABNT, 2005), a segurança da informação é definida como: "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

2.1 Os Três Pilares da Segurança da Informação

Pode-se definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças em cima de três pilares principais que são a integridade, a disponibilidade e a confidencialidade, conforme ilustrado pela Figura 2, a fim de garantir a continuidade do negócio e minimizar os riscos.

Figura 2 - Pilares da Segurança da Informação



Fonte: Ribeiro (2018)

A seguir são descritos os conceitos destes três pilares:

- **Integridade:** “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais” (SÊMOLA, 2013, p. 45). Ou seja, informação não adulterada.
- **Disponibilidade:** “Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna (BEAL, 2005, p. 1). Ou seja, independente da finalidade, a informação deve estar disponível.
- **Confidencialidade:** “Garantia de que o acesso à informação é restrito aos seus usuários legítimos.” (BEAL, 2005, p. 1). Ou seja, seu acesso é permitido apenas a determinados usuários.

Além destes, segundo Lyra (2008, p.4), podemos citar mais alguns aspectos complementares para garantia da segurança da informação:

- **Autenticação:** “Garantir que um usuário é de fato quem alega ser”.
- **Não repúdio:** “Capacidade do sistema de provar que um usuário executou uma determinada ação”.
- **Legalidade:** “Garantir que o sistema esteja aderente à legislação”.
- **Privacidade:** “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.
- **Auditoria:** “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.

Como visto, a Segurança da Informação é essencial para todos os setores da sociedade e estar 100% seguro é uma meta a ser perseguida e também um desafio, pois, se tratar da segurança pessoal já é difícil, imagine-se, então, tratar da segurança da informação, em que a evolução tecnológica é a cada dia mais veloz e não alcança toda uma sociedade em todos os seus níveis.

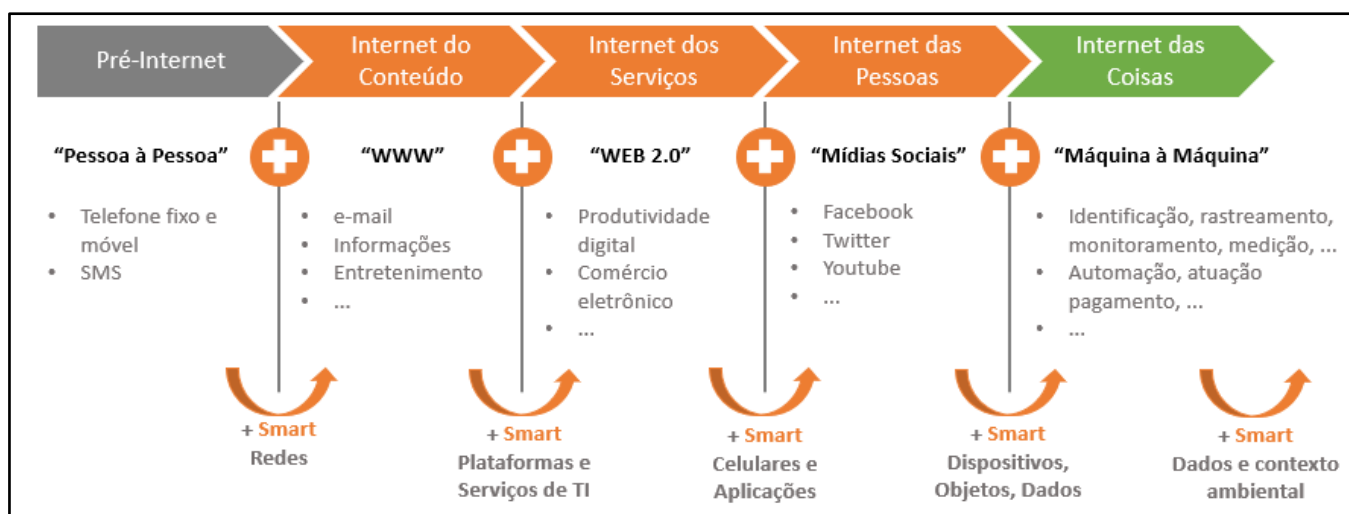
Neste contexto, nos capítulos seguintes, serão abordados os temas IoT e os desafios quanto a Segurança da Informação, e também como as ameaças encontradas podem ser mitigadas, possibilitando se beneficiar da melhor forma possível, dos recursos proporcionados por esta nova tecnologia.

3. A Internet das Coisas

A IoT trata-se de uma evolução tecnologia que possibilitou a interligação e conexão de objetos físicos, de forma inteligente, à Internet, com o objetivo de trocar, armazenar e coletar dados para consumidores e empresas, através de uma aplicação de *software* (CARRION; QUARESMA, 2019). Estes objetos, são geralmente dispositivos eletrônicos baseados em circuito integrado que podem enviar dados através de uma rede, podendo ser esta uma Rede de Sensores Sem Fio (RSSF) (GANESHAN, 2017).

O termo IoT foi usado pela primeira vez por Kevin Ashton, pesquisador britânico do Massachusetts Institute of Technology (MIT), como título de uma apresentação realizada no ano de 1999, para a empresa Procter & Gamble (P&G) sobre a aplicação da tecnologia de Identificação por Rádio Frequência (RFID) na cadeia de suprimentos desta empresa (ASTHON, 2009). O pesquisador menciona que os seres humanos e o ambiente que os cerca são físicos, já a sociedade e a economia são baseadas em coisas. "Porém a tecnologia atual dependem tanto dos dados gerados pelas pessoas que os computadores sabem mais sobre ideias do que sobre coisas" (ASTHON, 2009, p. 1). A Figura 3 ilustra a evolução da IoT.

Figura 3 - A Evolução da IoT



Fonte: Adaptado de Code for Billion (2017)

Na época a IoT era relacionada com o uso da tecnologia RFID e o termo ainda não era foco de grande número de pesquisas (SANTOS *et al.*, 2016). A IoT foi identificada como uma tecnologia emergente em 2012 por especialistas da área e foi previsto que levaria entre 5 e 10 anos para ser adotada pelo mercado (GARTNER, 2015). É esperado que até 2025 a IoT impacte a economia mundial em cerca de 11 trilhões de dólares, e o número de coisas conectadas, tais como comidas, roupas, móveis, papéis, monumentos, veículos automotivos, obras de arte, etc.; deverá crescer, chegando a 50,1 bilhões de coisas no ano em questão (COMPTIA, 2016).

Uma vez que a ideia da IoT, se tornou mais conhecida, seu conceito passou a ser referência para outros termos, tais como Internet física, computação ubíqua, comunicação M2M (Machine-to-Machine, ou Máquina-a-Máquina), Web of Things (ou Rede das Coisas), ambientes conectados, cidades inteligentes, redes de sensores sem fio, entre outros (CARRION; QUARESMA, 2019, p. 52). A Figura 4 ilustra as interações entre pessoas, máquinas e coisas, que ocorrem na IoT.

Figura 4 - Interações na IoT

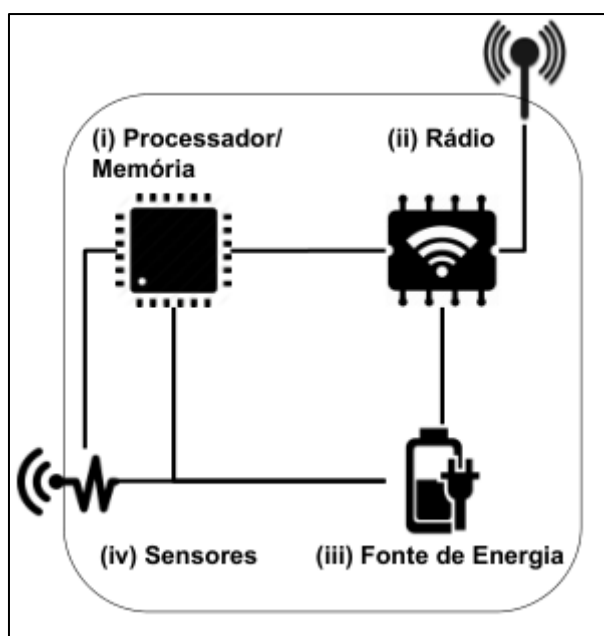


Fonte: Martin (2019)

3.1 Dispositivos e Tecnologia de Comunicação

Os dispositivos IoT são compostos basicamente por 4 elementos: processador/memória, interface de comunicação, fonte de energia e sensores/atuadores. A Figura 5 ilustra esta arquitetura e como estes elementos são interligados, os quais são descritos a seguir:

Figura 5 – Arquitetura dos Dispositivos IoT



Fonte: Santos *et al* (2016)

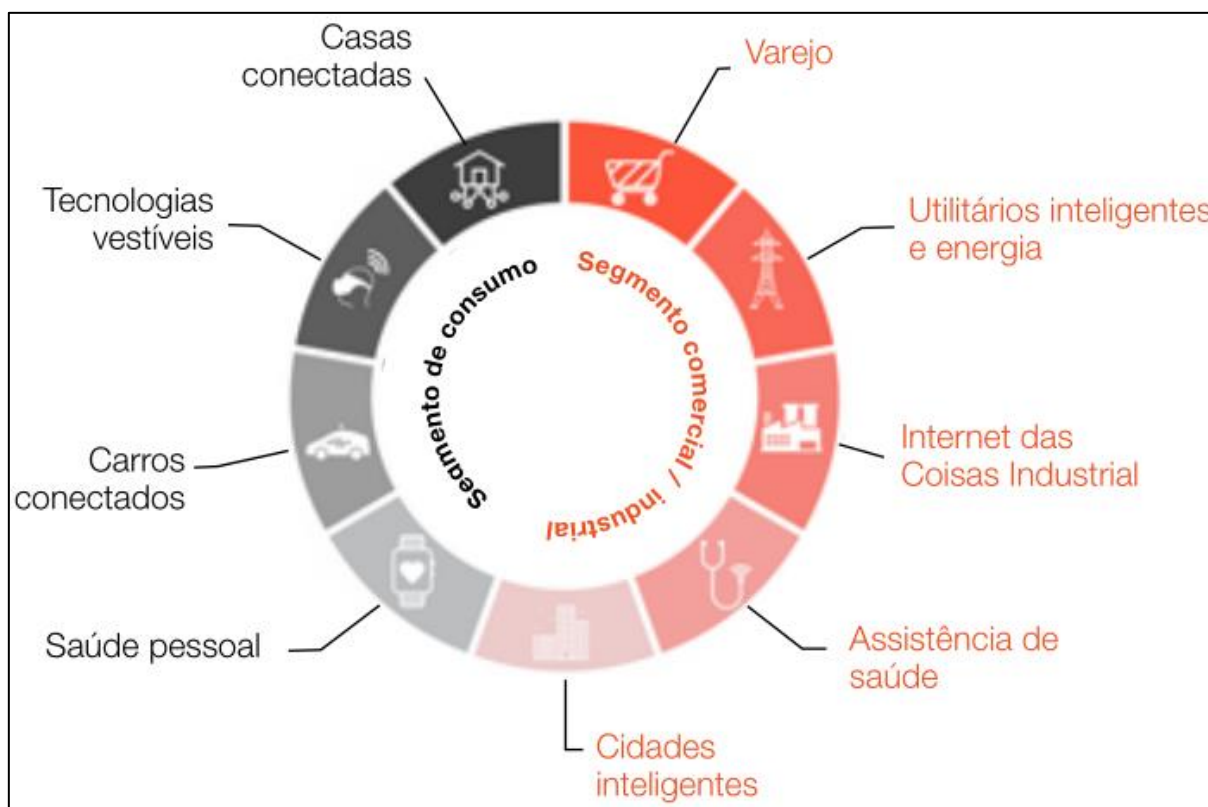
- **Processador/Memória:** Esta unidade é composta de uma memória interna para armazenamento de dados e programas, um microcontrolador e um conversor analógico-digital para receber sinais dos sensores. As CPUs utilizadas para os dispositivos são, em geral, as mesmas utilizadas em sistemas embarcados e comumente não apresentam alto poder computacional. Frequentemente existe uma memória externa do tipo flash, que serve como memória secundária, por exemplo, manter um “log” de dados. As características desejáveis para estas unidades são pouco consumo de energia e o componente deve ocupar o menor espaço possível.

- **Interface de Comunicação:** Esta unidade consiste de um canal de comunicação com ou sem fio, sendo mais comum o meio sem fio. Neste último caso, a maioria das plataformas usam rádio de baixa potência e custo. Como consequência, a comunicação é de curto alcance e apresentam perdas frequentes.
- **Fonte de Energia:** É responsável por alimentar os componentes do dispositivo IoT. Normalmente, a fonte de energia consiste de uma bateria recarregável (ou não) e um conversor AC/DC, entretanto, existem diversas outras fontes de alimentação como energia elétrica, solar entre outras.
- **Sensores ou Atuadores:** Estes elementos são responsáveis por interagir com o ambiente em que o dispositivo está imerso. Os sensores são responsáveis por lidar com grandezas físicas como temperatura, umidade, pressão, presença, etc. Os atuadores são dispositivos que produzem movimento, atendendo a comandos que podem ser manuais, elétricos ou mecânicos.

3.2 Benefícios da Tecnologia IoT

O desenvolvimento da tecnologia IoT tem dois objetivos básicos que são: atender consumidores domésticos e explorar a digitalização de setores industriais. No cenário doméstico, a IoT é caracterizada pelo uso de “coisas” e sensores conectados à Internet, como eletrodomésticos, televisores, aparelhos de som, smartphones, roteadores e automóveis, e essa utilização é intermediada por diversos serviços, como aplicativos de transporte, aplicativos de tráfego urbano e também serviços bancários. Já a utilização comercial e industrial é marcada pela promessa de cidades inteligentes, monitoramento de pacientes em hospitais, aprimoramento na gestão de recursos energéticos e do setor de saúde, entre outros (HUREL; LOBATO, 2018). A Figura 6 ilustra a utilização da IoT no mercado doméstico, comercial e industrial.

Figura 6 - Panorama do Mercado de IoT



Fonte: Adaptado de Hurel e Lobato (2018)

Os benefícios na utilização das tecnologias IoT em larga escala são impulsionados pela Indústria 4.0 e se fundamentam nas seguintes ideias (HUREL; LOBATO, 2018, p. 7):

- incorporação de sensores à produtos e equipamentos de manufatura;
- proliferação de sistemas ciber-físicos;
- análise de dados em grande escala.

E são habilitados pelos seguintes processos:

- Convergência entre dados, poder computacional e conectividade, entre IoT, computação na nuvem e Big Data. Essa junção torna possível o uso ubíquo de sensores e uma redução nos custos de processamento transmissão e armazenamento de dados;

- Análise e inteligência de dados, viabilizada por avanços na inteligência artificial e no aprendizado de máquina (Machine Learning). Isto beneficia os processos de digitalização e automação, e também o desenvolvimento de métodos sofisticados de análise e estatística;
- Interação entre humanos e máquinas (Human to Machine), caracterizada principalmente pelo uso de dispositivos pessoais com interfaces sensíveis ao toque, reconhecimento de gestos e realidade aumentada;
- Conversão digital para o físico, representada pela robótica avançada e sistemas de impressão 3D. Uma combinação de custos mais baixos, disponibilidade de materiais diversos e avanços na precisão e qualidade são motores desse processo.

Como visto, a IoT fornece uma solução capaz de trazer melhoria para a vida das pessoas ao possibilitar a troca de dados entre máquinas, facilitando o acesso à informação e ainda promovendo a economia de energia, saúde, educação, entre outros aspectos do cotidiano. No meio industrial pode aumentar a produtividade, criar novas estratégias de produção e também permitir conhecer melhor o mercado. Em termos gerais, a IoT busca eliminar a necessidade de intervenção humana em diversos aspectos, facilitando ao mesmo tempo a vida de quem a utiliza.

3.3 Principais Desafios

A IoT possibilita uma nova gama de aplicações das quais tanto os consumidores domésticos quanto a indústria, podem se beneficiar (SANTOS *et al.*, 2016). Porém novos desafios emergem junto com esta tecnologia, e é necessário conhecê-los e entendê-los a fim de se obter um melhor planejamento na sua implantação e utilização.

Neste capítulo serão abordados, no ponto de vista de Hurel e Lobato (2018), os cinco principais desafios que foram identificados durante a pesquisa do trabalho que são: Armazenamento, Conectividade, Energia, Padronização, Segurança / Privacidade, os quais serão detalhados a seguir:

3.3.1 Armazenamento

Os dispositivos IoT geram uma imensa quantidade de dados provenientes da coletas e monitoramento que estes dispositivos realizam, e é necessário que haja uma estrutura capaz de armazená-los, além de garantir sua privacidade e que não sejam violados, já que muitos destes dados podem conter informações confidenciais e sensíveis.

3.3.2 Conectividade

Com a ampliação no uso da IoT, novos dispositivos estão sendo conectados à Internet a todo momento e cada um desses dispositivos necessita de um endereçamento individual na rede. O protocolo IPV4, utilizado até então, já não possui mais disponibilidade de endereços, sendo necessário a migração para o protocolo IPV6, que possui uma capacidade muito superior de endereçamento o que possibilita atender a grande demanda gerada pela IoT.

3.3.3 Energia

Dispositivos IoT precisam de energia para funcionar e esta é uma outra questão importante já que a energia utilizada muitas vezes é proveniente de uma bateria acoplada e sua substituição pode ser dificultada pelo acesso físico. É importante que

sejam avaliadas formas de geração de energia autossustentáveis, utilizando elementos ambientais como vibração, luz, temperatura, entre outros, e também sejam utilizados recursos de gerenciamento inteligente de energia, como por exemplo, redução de atividade ou suspensão em momentos de ociosidade dos dispositivos.

3.3.4 Padronização

Um grande número de objetos inteligentes com interfaces, serviços, e capacidades computacionais próprias tem surgido no mercado, sendo crucial a interoperabilidade entre esses objetos e seu entorno. A falta de padrões compartilhados pode se tornar um grande obstáculo para a segurança, resiliência e estabilidade da IoT, já que grande parte dos objetos, softwares e soluções se baseiam em tecnologias com diferentes padrões técnicos. A padronização permite que a heterogeneidade de dispositivos conectados à Internet cresça, tornando possível a implementação da IoT.

3.3.5 Segurança / Privacidade

O comportamento autônomo dos dispositivos IoT, pode trazer prejuízo ao ambiente onde estão atuando, caso não estejam adequadamente protegidos. Devido ao baixo poder computacional que a maioria destes dispositivos possuem, dificuldades podem ser encontradas na implementação de medidas de segurança como criptografia, senhas e também na utilização de algoritmos mais sofisticados. Outro ponto que deve ser levado em consideração é que com a utilização da comunicação sem fio, várias vulnerabilidades conhecidas desta tecnologia são agravadas pela dificuldade na utilização de uma criptografia robusta, comprometendo as propriedades básicas da segurança da informação como a disponibilidade, integridade, confidencialidade e privacidade.

Como visto, são vários os desafios para a implantação definitiva da IoT e pode-se afirmar que a segurança da informação é o principal obstáculo dentre eles, pois é o que oferece maior dificuldade de ser resolvido, já que não existem sistemas e dispositivos 100% seguros (MORAES, 2010). Porém o entendimento das vulnerabilidades e a forma como os ataques são realizados, possibilitam planejar a

implantação da IoT de forma a maximizar a proteção dos dados coletados e minimizar os riscos de ataques cibernéticos.

No próximo capítulo serão apresentadas as questões sobre vulnerabilidades e tipos de ataques em ambientes IoT e também os métodos que podem ser utilizados para impedir ou minimizar os efeitos dos mesmos.

4. SEGURANÇA DA INFORMAÇÃO NA IoT

Como visto nos capítulos anteriores, a IoT promete um aumento de investimentos em tecnologias avançadas no setor privado e integração de objetos interconectados nas atividades comuns das organizações e pessoas, porém surgem novos desafios com reação à segurança da informação e à privacidade dos dados coletados (HUREL; LOBATO, 2018).

De acordo com o Relatório Global de Riscos de 2018, do Fórum Econômico Mundial, organização sem fins lucrativos com sede em Genebra, ataques cibernéticos são a terceira maior ameaça global, logo depois de desastres naturais, como pode ser visto na Figura 7 (WORLD ECONOMIC FORUM, 2018).

Figura 7 - Relatório Global de Riscos

Os 10 principais riscos em termos de Probabilidade	Os 10 principais riscos em termos de Impacto	Categorias
1 Eventos Climáticos Extremos	1 Armas de Destruição em Massa	Riscos Econômicos
2 Desastres Naturais	2 Eventos Climáticos Extremos	Riscos Ambientais
3 Ataques Cibernéticos	3 Desastres Naturais	Riscos Geopolíticos
4 Fraude ou Roubo de Dados	4 Incapacidade de Adaptação e Mitigação de Mudanças	Riscos Sociais
5 Incapacidade de Adaptação e Mitigação de Mudanças	5 Crises de abastecimento de águas	Riscos Tecnológicos
6 Migração Involuntária em Grande Escala	6 Ataques Cibernéticos	
7 Desastres ambientais provocados pelo homem	7 Crises Alimentares	
8 Ataques Terroristas	8 Perda de Biodiversidade e Colapso do Ecossistema	
9 Comércio Ilícito	9 Migração Involuntária em Larga Grande	
10 Bolhas de Ativos em uma Grande Economia	10 Disseminação de Doenças Infecciosas	

Fonte: Adaptado de *World Economic Forum* (2018)

Ataques e vazamento de dados de dispositivos conectados, tais como torradeiras, geladeiras e até mesmo babá eletrônica inteligente, expõem o consumidor a um ecossistema de dispositivos e sensores que coletam dados indiscriminadamente

e atualmente, somente 1% dos dados coletados por esses objetos e sensores são, de fato, utilizados (HUREL; LOBATO, 2018).

Enquanto as pessoas desconhecem os tipos de dados que estão sendo coletados e como estão sendo compartilhados, as empresas buscam maximizar o seu aproveitamento. Neste cenário, os objetos conectados se tornam grandes alvos de ataques cibernéticos, causando impactos negativos nas redes onde estão conectados, à Internet e conseqüentemente a outros setores da sociedade (HUREL; LOBATO, 2018).

A grande maioria dos problemas relacionados à segurança em uma rede de computadores também se aplicam aos dispositivos IoT. Alguns destes problemas, inclusive, são bem mais críticos, devido a maioria destes dispositivos apresentarem limitações de hardware e também, devido ao meio de comunicação que eles utilizam, que geralmente é a sem fio (ANDREA; CHRYSOSTOMOU; HADJICHRISTOFI, 2015).

O objetivo de segurança mais desejável da IoT é proteger os dados coletados, já que os dados coletados de dispositivos físicos também podem incluir informações confidenciais do usuário. Por esse motivo, a segurança de qualquer sistema de IoT precisa ser resiliente a ataques relacionados a dados e fornecer confiança, segurança e privacidade de dados.

Sendo assim, a Segurança da Informação é um objetivo que deve ser buscado de forma constante pois, segundo o autor Moraes (2010), não existe rede ou mesmo informação 100% segura. Todas as vezes que alguma informação é disponibilizada e transmitida através de uma rede, os riscos existem.

4.1 Vulnerabilidades Possíveis em Ambientes IoT

O surgimento de novos dispositivos dedicados a IoT tem causado grande preocupação nos fabricantes, usuários corporativos e consumidores, pelo fato dos mesmos poderem ser comprometidos. O problema se torna mais crítico pois dispositivos vulneráveis podem ser invadidos e utilizados em *botnets*, além disso podem prejudicar até mesmo redes adequadamente protegidas. A fim de mitigar os possíveis problemas de segurança que possam ocorrer na implantação e utilização

da tecnologia IoT, se faz necessário conhecer e entender as vulnerabilidades presentes atualmente nestes dispositivos (PAUL, 2019).

Uma vulnerabilidade ou falha em uma rede pode ocorrer por vários fatores, como, por exemplo, um problema em uma aplicação, um serviço, ocorrência de um vírus, ou ainda, um usuário que divulga a senha indiscriminadamente (CERT.BR, 2012). Existem também ameaças mais perigosas, como alguém que sabota a base de dados de uma empresa por vingança, ou mesmo por um espião contratado para obter informações importantes da empresa através de sua rede (MORAES, 2010).

A OWASP (Open Web Application Security Project) ou Projeto Aberto de Segurança em Aplicações Web é uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web (OWASP, 2018). Com o objetivo de ajudar fabricantes, desenvolvedores e consumidores a entender melhor as questões de segurança associadas à IoT, surgiu o projeto OWASP Internet of Things, permitindo que usuários, em qualquer contexto, tomem as melhores decisões de segurança ao criar, implantar ou avaliar tecnologias de IoT (OWASP, 2018).

No fim de 2018, a OWASP (2018), divulgou uma lista com as 10 principais vulnerabilidades de IoT para 2019, as quais estão descritas a seguir:

4.1.1 Senhas fracas, previsíveis ou dentro do código

Uso de senhas que não podem ser modificadas e que estão publicamente disponíveis ou são fáceis de adivinhar através da utilização da técnica de força bruta, e até mesmo de *backdoors* em *firmware* ou *software* cliente que permitem obter acesso não autorizado a sistemas, aproveitando-se dessas senhas vulneráveis.

4.1.2 Serviços de rede inseguros

Serviços de rede inseguros e desnecessários em execução no próprio dispositivo, especialmente aqueles expostos à Internet, que comprometem a confidencialidade, autenticidade ou disponibilidade de informações ou permitem o controle não autorizado de forma remota.

4.1.3 Ecossistema de interfaces inseguros

Problemas de segurança em interfaces web, móveis, na nuvem, ou API (Application Programming Interface) de *backend* em ecossistemas que estão fora dos dispositivos e que permitem que tanto os dispositivos como certos componentes relacionados possam ser comprometidos.

4.1.4 Falta de mecanismos de atualização seguros

A falta de um sistema simples para atualizar o dispositivo de forma segura. Isso inclui: falta de validação do *firmware* no dispositivo, falta de segurança no envio (tráfego não criptografado), falta de mecanismos para evitar voltar atrás e falta de notificações sobre alterações de segurança devido às atualizações.

4.1.5 Uso de componentes inseguros ou obsoletos

Uso de componentes/bibliotecas de software obsoletos e/ou inseguros que podem permitir que o dispositivo seja comprometido. Isso inclui a personalização insegura da plataforma do sistema operacional e o uso de software de terceiros ou componentes de hardware de uma cadeia de suprimentos comprometida.

4.1.6 Proteção da privacidade insuficiente

Informações pessoais do usuário armazenadas no dispositivo ou no ambiente ao qual o dispositivo está conectado, usadas de maneira insegura, inadequada ou sem permissão.

4.1.7 Transferência e armazenamento de dados de maneira insegura

Falta de criptografia ou controle de acesso para dados confidenciais que estão dentro do ecossistema, incluindo dados em repouso, em trânsito ou em processamento.

4.1.8 Falta de controle de gerenciamento dos dispositivos

Falta de suporte de segurança em dispositivos liberados para produção, incluindo gerenciamento de ativos, gerenciamento de atualizações, desarme seguro, monitoramento de sistemas e recursos de resposta.

4.1.9 Configuração insegura por padrão

Dispositivos ou sistemas com configurações padrão pouco seguras ou sem a possibilidade de tornar o sistema mais seguro, aplicando restrições com base nas alterações de configuração.

4.1.10 Segurança física insuficiente

Falta de medidas que permitam fortalecer os dispositivos desde o ponto de vista físico, o que faz com que cibercriminosos possam ter acesso a informações confidenciais que podem ser úteis em um futuro ataque remoto ou para assumir o controle local do dispositivo.

O rápido crescimento no número de dispositivos interconectados e sua difusão no mercado apresentam desafios tecnológicos e o principal deles consiste na pouca importância atribuída à privacidade e à segurança por concepção. Sendo assim, é necessário entender que a IoT é uma implementação de tecnologias de redes e uma integração de infraestruturas de redes existentes, por tanto, todos os desafios e ameaças à segurança de cada tecnologia de rede são passados por padrão para os sistemas IoT que utilizam essas tecnologias. Por esse motivo, a segurança de qualquer sistema de IoT precisa ser resiliente a ataques relacionados a dados e físico, fortalecendo a confiança, segurança e privacidade das informações que são compartilhadas neste ecossistema.

4.2 Ataques Possíveis em Ambientes IoT

Com os avanços tecnológicos decorrente da exploração da IoT, novas maneiras e oportunidades de ataques cibernéticos também tendem a surgir. A medida que cresce a quantidade de dispositivos conectados e que podem ser acessados, também aumenta a extensão dos danos que podem ser causados. E com essa grande quantidade de dispositivos, menor é o controle sobre quais deles possuem as últimas medidas de segurança atualizadas.

Andrea, Chrysostomou e Hadjichristofi (2015), classificaram os ataques a IoT em quatro categorias distintas como: ataques físicos, de rede, de software e de criptografia, os quais serão detalhados nos tópicos seguintes.

4.2.1 Ataques Físicos

Esta categoria de ataque está focada nos componentes de hardware do sistema de IoT, conhecidos também como NS (Nó Sensor) o invasor precisa ter acesso físico aos dispositivos para que os ataques sejam bem-sucedidos. Além disso, ataques que prejudicam a vida útil ou o funcionamento do hardware, também estão inclusos. Esta categoria está subdividida em 8 tipos de ataques, os quais são descritos a seguir:

- **Adulteração de NS:** O invasor pode causar danos ao NS, ao substituir fisicamente todo o NS ou parte de seu hardware ou mesmo corromper eletronicamente os NSs para obter acesso e alterar informações confidenciais, como chaves criptográficas compartilhadas (se houver), tabelas de roteamento, ou impactar a operação das camadas de comunicação.
- **Interferência por radiofrequência em sistemas RFIDs:** Um ataque DoS pode ser implementado em qualquer sistema RFID, criando e enviando sinais de ruído através da mesma radiofrequência utilizada pelo sistema RFID. Os sinais de ruído causaram interferências e dificultaram a comunicação.

- **Bloqueio do NS em RSSF:** É semelhante ao ataque de interferência por radiofrequência em sistemas RFIDs, com a diferença de que este ataque é baseado em RSSF. O atacante pode causar interferência nas frequências utilizadas pelo NS, bloqueando os sinais e não permitindo a comunicação entre os nós. Se o atacante conseguir obstruir a comunicação dos principais NSs, ele poderá negar com êxito o serviço de IoT.
- **Injeção de NS Malicioso:** O invasor pode implantar fisicamente um NS malicioso entre dois ou mais NSs no sistema de IoT e assim poderá controlar todo o fluxo de dados da rede e sua operação. Este tipo de ataque também é conhecido como MITM (Man in The Middle).
- **Danos físicos:** O invasor pode danificar fisicamente os dispositivos da rede IoT para seu próprio benefício. Este é um tipo de ataque que está relacionado com a segurança física da área ou prédio onde o sistema IoT está instalado. Difere do ataque de adulteração de NS, pois neste caso o invasor tenta danificar diretamente o sistema de IoT, com o objetivo de impactar a disponibilidade do serviço.
- **Engenharia social:** O invasor manipula usuários de um sistema de IoT, para extrair informações particulares ou executar determinadas ações a fim de atingir seus objetivos. Esse tipo de ataque está inserido na categoria de Ataques Físicos, pois o invasor precisa interagir fisicamente com os usuários da rede de IoT.
- **Ataques de negação de suspensão de atividade:** A maioria dos dispositivos no sistema IoT são alimentados por baterias substituíveis e estão programados para seguir rotinas de suspensão de atividade, afim de prolongar a vida útil das baterias. Esse ataque mantém os dispositivos ativos, resultando em um maior consumo de energia e consequentemente tornando o dispositivo indisponível assim que a carga da bateria esgotar.

- **Injeção de código malicioso:** O invasor pode comprometer um NS, injetando fisicamente um código malicioso que lhe concederia acesso ao sistema de IoT.

4.2.2 Ataques de Rede

Nesta categoria, os ataques estão centralizados na rede do sistema de IoT e o invasor não precisa necessariamente estar perto fisicamente da rede para efetuar o ataque. Esta categoria está subdividida em 9 tipos de ataques, os quais são descritos a seguir:

- **Ataques de Análise de Tráfego:** Um invasor pode detectar as informações confidenciais ou quaisquer outros dados provenientes das tecnologias RFID devido a suas características sem fio. Além disso, em quase todos os ataques, um invasor primeiro tenta obter algumas informações sobre a rede antes de efetuar seu ataque. Esta ação é realizada usando aplicações de *sniffing*, escaneamento de portas e *sniffer* de pacotes.
- **Falsificação de RFID:** Neste tipo de ataque, um invasor falsifica sinais de RFID para ler e gravar uma transmissão de dados a partir de um dispositivo. O invasor então envia seus próprios dados contendo a ID do dispositivo original, tornando o sinal falsificado válido, deste modo, o invasor obtém acesso total ao sistema fingindo ser a fonte original.
- **Clonagem de RFID:** Um invasor clona um dispositivo RFID copiando os dados das vítimas para outros dispositivos RFID. Embora os dois dispositivos passem a ter dados idênticos, esse método não replica o ID original do RFID, tornando possível distinguir entre o original e o comprometido, diferentemente do evento no ataque de falsificação de RFID.
- **Acesso não autorizado a dispositivos RFID:** Devido à falta de mecanismos de autenticação adequados na maioria dos sistemas RFID,

os dispositivos podem ser acessados por qualquer pessoa. Isso permite que ao invasor ler, modificar ou até mesmo excluir dados nos dispositivos.

- **Sinkhole (Buraco Negro):** O invasor atrai todo o tráfego dos NS da RSSF, criando um "buraco negro". Esse tipo de ataque viola a confidencialidade dos dados e também nega serviço à rede descartando todos os pacotes em vez de encaminhá-los para o destino desejado.
- **Ataques MITM:** Neste tipo de ataque, o invasor consegue interferir entre dois NSs, acessando dados restritos, violando a privacidade, monitorando, interceptando e controlando a comunicação entre os mesmos. Diferente da Injeção de código malicioso, da categoria “Ataques Físicos”, o invasor não precisa estar fisicamente no local onde está o dispositivo para que esse tipo de ataque seja realizado, apenas depende dos protocolos de comunicação da rede de um sistema IoT.
- **Ataques de negação de serviço (DoS):** Um invasor pode bombardear uma rede IoT com mais dados de tráfego que ela pode gerenciar, o que pode resultar em um ataque de negação de serviço.
- **Ataques de informações de roteamento:** São ataques diretos no qual o invasor falsificando, alterando ou reproduzindo informações de roteamento pode complicar a rede e criar loops de roteamento, permitindo ou descartando tráfego, enviando mensagens de erro falsas, encurtando ou estendendo rotas de origem ou até particionando a rede. Exemplo: Ataques *Hello* e *Blackhole*.
- **Ataques Sybil:** Este tipo de ataque caracteriza-se pela manipulação de identidades falsas ou “roubadas”. Os usuários maliciosos realizam este ataque explorando as vulnerabilidades das redes, como a interceptação de pacotes. Sendo assim, a ocorrência de ataques *Sybil* nos sistemas presentes na IoT afeta em relatórios equivocados, sistemas de votação, acesso indevido a um conteúdo entre outros males.

4.2.3 Ataques de *Software*

Segundo Andrea, Chrysostomou e Hadjichristofi (2015), os ataques de *software* são a principal fonte de vulnerabilidade de segurança em qualquer sistema computadorizado. Esses ataques exploram o sistema usando *trojans*, *worms*, vírus, *spyware* e *scripts* maliciosos que podem roubar informações, adulterar dados, negar serviço e até danificar os dispositivos de um sistema de IoT. Esta categoria está subdividida em 4 tipos de ataques, os quais são descritos a seguir:

- **Ataques de *phishing*:** O invasor obtém acesso a dados confidenciais falsificando as credenciais de autenticação de um usuário, geralmente através de e-mails infectados ou sites de *phishing*.
- **Vírus, Worms, Trojans Spyware e Adwares:** Um invasor pode infectar o sistema com software malicioso, ocasionando uma variedade de resultados como roubo de informações, adulteração de dados ou mesmo negação de serviço.
- **Scripts maliciosos:** Geralmente as redes IoT estão conectadas à Internet. O usuário que controla o *gateway* pode ser enganado ao executar *scripts*, podendo resultar em um desligamento completo do sistema ou em roubo de dados.
- **Negação de serviço (DoS):** Um invasor pode executar ataques de DoS ou DDoS na rede IoT, por meio da camada de aplicação, afetando todos os usuários da rede. Esse tipo de ataque também pode bloquear os usuários legítimos e fornecer acesso completo aos bancos de dados confidenciais.

4.2.4 Ataques de Criptografia

Nesta categoria, os tipos de ataques são baseados exclusivamente na quebra do esquema de criptografia usado em um sistema de IoT. Esta categoria está subdividida em 3 tipos de ataques, os quais são descritos a seguir:

- **Ataques de canal lateral:** Usando técnicas de análise específicas de sincronização de informações, consumo de energia, vazamentos eletromagnéticos e até sons, dos dispositivos de criptografia de um sistema IoT, o invasor pode recuperar a chave de criptografia usada para criptografar e descriptografar os dados compartilhados na rede.
- **Análises de criptografia:** Neste tipo de ataque o invasor possui acesso ao texto cifrado ou ao texto simples e seu objetivo é encontrar a chave de criptografia que está sendo utilizada através da quebra do método de criptografia do sistema. Exemplos de ataques de criptoanálise em sistemas de IoT incluem ataque de texto simples conhecido, ataque de texto simples escolhido, ataque de texto cifrado escolhido e ataque somente de texto cifrado.
- **Ataques MITM:** Quando dois usuários A e B de um sistema IoT trocam chaves durante um cenário de desafio-resposta, de modo a estabelecer um canal de comunicação seguro, um invasor se posiciona entre eles no canal de comunicação. O invasor intercepta os dados que A e B enviam um ao outro e tenta interferir executando uma troca de chaves com A e B separadamente. O invasor poderá, então, descriptografar / criptografar quaisquer dados provenientes de A e B com as chaves que ele compartilha com os dois. A e B pensam que estão conversando entre si.

Um resumo da classificação destes ataques é mostrado na Tabela 1:

Tabela 1 - Classificação dos Ataques a IoT

Ataques Físicos	Ataques de Rede	Ataques de Software	Ataques de Criptografia
Adulteração de nós	Ataques de análise de tráfego	Ataques de phishing	Ataques de canal lateral
Interferência por RF	Falsificação de RFID		
Bloqueio de nós	Clonagem de RFID	Vírus, Worms, Trojans, Spyware e Adwares	Ataques de criptoanálise: a) Ataque exclusivo a textos cifrados b) Ataque a textos simples conhecidos c) Ataque a textos simples ou cifrados selecionados
Injeção de nó malicioso	Acesso não autorizado a dispositivos RFID		
Danos físicos	Sinkhole	Scripts maliciosos	
Engenharia social	Ataques man in the middle		
Ataques de negação de suspensão de atividade	Ataques de negação de serviço	Negação de serviço	Ataques Man In the Middle
Injeção de código malicioso			

Fonte: Adaptado de Andrea, Chrysostomou e Hadjichristofi (2015)

Ainda não há soluções definitivas para todos os ataques que a IoT pode sofrer, porém existem medidas de defesa que podem mitigar esses ataques e reduzir os impactos que os mesmos possam causar (ANDREA; CHRYSOSTOMOU; HADJICHRISTOFI, 2015).

No capítulo seguinte são apresentados os principais métodos que podem ser utilizados para impedir ou minimizar os efeitos de uma possível invasão em um sistema IoT.

4.3 Principais Métodos de Segurança para IoT

Como visto no tópico anterior, um sistema IoT consiste em três camadas diferentes, sendo elas: Física, Rede e Aplicação, e cada uma possui vulnerabilidades específicas possibilitando ataques de segurança (ANDREA; CHRYSOSTOMOU; HADJICHRISTOFI, 2015). Na Tabela 2 está um resumo da abordagem em segurança da IoT em várias camadas realizada pelos mesmos autores.

Tabela 2 - Medidas de Contra-Ataque para IoT

Camadas da IoT	Medidas de contra-ataques para a camada específica	Medidas de contra-ataques para todas as camadas
Camada Física	<ol style="list-style-type: none"> 1) Inicialização segura para todos os dispositivos IoT <ol style="list-style-type: none"> a) Funções de hash criptográfico de baixa potência 2) Autenticação de dispositivo usando técnicas de baixa potência <ol style="list-style-type: none"> a) Integridade dos dados b) Verificação cíclica de redundância (CRC) c) Checsun d) Bit de paridade e) Função de hash criptográfico WH 3) Confidencialidade dos dados <ol style="list-style-type: none"> a) Algoritmos de criptografia como Blowfish e RSA 4) Anonimato dos dados <ol style="list-style-type: none"> a) K-Anonimato 	<ol style="list-style-type: none"> 1) Avaliação de riscos <ol style="list-style-type: none"> a) Encontrar novas ameaças b) Aplicar atualizações c) Aplicar correções de segurança d) Fornecer melhorias 2) Mecanismos de detecção de invasão específico para sistemas IoT 3) Proteção para as instalações da IoT <ol style="list-style-type: none"> a) Barreiras físicas b) Alarmes de detecção de invasão c) Dispositivos de monitoramento d) Dispositivos de controle de acesso e) Segurança Patrimonial 4) Políticas de segurança da informação <ol style="list-style-type: none"> a) Segurança entre camadas b) Confiabilidade e privacidade entre as camadas c) Confiabilidade entre a IoT e o usuário
Camada de Rede	<ol style="list-style-type: none"> 1) Comunicação segura entre os dispositivos <ol style="list-style-type: none"> a) Autenticação de rede - mecanismos de desafio-resposta b) Criptografia ponto a ponto para a confidencialidade dos dados transmitidos c) Funções de hash criptográfico para a integridade dos dados transmitidos 2) Implementação da segurança de roteamento <ol style="list-style-type: none"> a) Uso de várias rotas b) Tabelas criptografadas de roteamento c) Tabelas hash de roteamento 3) Proteger dados do usuário nos dispositivos <ol style="list-style-type: none"> a) Autenticação de dados b) Confidencialidade dos dados; Esquemas de criptografia c) Integridade dos dados; Funções de hash criptográfico 	
Camada de Aplicação	<ol style="list-style-type: none"> 1) Segurança de Dados <ol style="list-style-type: none"> a) Autenticação; Biometria; Senhas; etc. b) Confidencialidade; Esquemas de criptografia forte (AES) c) Integridade; Funções de hash criptográficos 2) Listas de controle de acesso (ACLs) 3) Firewalls 4) Software de proteção <ol style="list-style-type: none"> a) Antivírus b) Anti-advare 	

Fonte: Adaptado de Andrea, Chrysostomou e Hadjichristofi (2015)

Ainda segundo os mesmos autores, para garantir a proteção contínua em um sistema IoT e manter sua confiabilidade, quatro itens devem ser considerados obrigatórios em todas essas as camadas:

- **Avaliação de riscos:** É fundamental para a segurança contínua do sistema, descobrir novas ameaças e aplicar atualizações e patches de correção ao *firmware* nos dispositivos conectados à rede, além de fornecer melhorias na estrutura de segurança existente

- **Detecção de invasão:** Os mecanismos de detecção de invasão nas três camadas da IoT (aplicação, rede e física) são muito importantes, pois alertariam o usuário sobre a ocorrência de qualquer atividade suspeita em qualquer uma destas três camadas;
- **Segurança física:** Proteger as instalações é talvez o recurso de segurança mais importante que a IoT precisa, pois é uma forma de garantir a integridade física dos dispositivos, sejam eles, NSs, computadores, firewalls, servidores de dados etc. A segurança dos dispositivos IoT é alcançada usando **barreiras físicas** para bloquear pessoas não autorizadas, **sistemas de detecção de invasão** para monitorar qualquer comportamento anormal, **controle de acesso** para garantir que apenas usuários autorizados entrem nas instalações da IoT e até mesmo utilização de **segurança patrimonial**, a fim de garantir a total segurança física dos dispositivos IoT.
- **Política de segurança da informação:** Uma política de segurança da informação precisa ser criada para garantir a confiabilidade de todo o sistema de IoT ao longo de sua execução. A entidade responsável pelo gerenciamento da política de segurança garantirá que as metas de segurança sejam cumpridas e que os mecanismos de segurança sejam implantados com sucesso.

Além destes itens, pesquisas devem ser realizadas para criar novos mecanismos seguros de criptografia e autenticação para dispositivos de ultrabaixa potência, e também novos protocolos de segurança devem ser desenvolvidos para atender os requisitos de segurança dos dispositivos IoT.

Os autores Shelby e Bormann (2011), complementam que para que um sistema IoT seja seguro é necessário estabelecer quais são os objetivos de segurança desejáveis, sendo que existem ao menos três grupos de objetivos desejáveis para segurança em IoT:

- **Confidencialidade:** neste requisito os dados transmitidos podem somente ser “escutados” e entendidos por elementos participantes da comunicação;
- **Integridade:** os dados não podem ser alterados por elementos da rede sem a devida autorização. É comum que hackers adulterem mensagens sem deixar vestígios e a quebra da integridade passe despercebida. De modo geral, implementa-se integridade criptografando as mensagens e as verificando no lado do receptor;
- **Disponibilidade:** deseja-se manter o sistema sempre disponível e seguros contra-ataques maliciosos. Entretanto, as redes sem fio estão sujeitas a interferências de comunicação e “hackers” podem agir nesta vulnerabilidade. Neste sentido, o sistema IoT deve ser capaz de identificar e tratar problemas como este para evitar ataques do tipo DoS.

Neste capítulo foram apresentados os principais aspectos de segurança e privacidade relacionados à IoT, teve-se um resumo do que é segurança, foram citados vários tipos de ataques que podem afetar as redes IoT e algumas contramedidas que podem ser tomadas para melhorar a segurança dos dispositivos. No próximo capítulo será feita uma abordagem sobre as boas práticas para implementação da IoT, com foco na segurança da Informação.

5. BOAS PRÁTICAS NA IMPLEMENTAÇÃO DA IOT

Atualmente, muitas pesquisas relacionadas à segurança digital dos dispositivos IoT estão sendo realizadas (CSA, 2016), porém nem todas as vulnerabilidades são corrigidas antes de um invasor explorá-las. As consequências de um vazamento de informações confidências, devido a um determinado dispositivo IoT que foi comprometido, podem ser catastróficas tanto para o usuário como para o fornecedor do equipamento pois além de possíveis danos físicos e prejuízos que possam causar ao usuário, o fornecedor do equipamento pode sofrer ações legais por conta das vulnerabilidades do dispositivo fornecido.

O objetivo deste capítulo é ser um guia de referência com orientações para o projeto e desenvolvimento de dispositivos IoT razoavelmente seguros, a fim corroborar com aqueles que desejarem se aprofundar nesta área.

5.1 Casos de Invasões Documentados

Neste tópico serão apresentados três casos de vulnerabilidades encontradas em dispositivos IoT utilizados atualmente, com o objetivo de exemplificar e alertar sobre os riscos e consequências que dispositivos vulneráveis podem causar na vida das pessoas e também das empresas.

5.1.1 Lâmpadas inteligentes podem estar vulneráveis a ataques de hackers

As lâmpadas inteligentes dispõem de diversas funcionalidades, que permitem controlar, por exemplo, a intensidade e a cor da luz, além de definir o horário para ligar e apagar podendo ser personalizada de acordo com a rotina do usuário e ainda possuem a vantagem de economizar energia (TECHTUDO, 2019). A Figura 8 mostra um exemplo de lâmpada inteligente, fabricada pela empresa brasileira Positivo.

Figura 8 - Lâmpada Inteligente Positivo



Fonte: Positivo Casa Inteligente (2019)

Uma pesquisa publicada pela Universidade do Texas, em outubro de 2019, revelou que existem alguns modelos de lâmpadas com vulnerabilidades que possibilitam ataques de hackers. A pesquisa identificou que algumas lâmpadas inteligentes se conectam diretamente a rede Wi-Fi, e devido a brechas de segurança em seu *firmware*, possibilitam que *hackers* tenham acesso a rede onde o dispositivo está conectado, permitindo o “roubo” de dados como textos, imagens ou qualquer outro arquivo do usuários que estejam em circulação na mesma rede, além de possibilitar a falsificação de outros dispositivos da casa. O estudo também alertou para o recurso de comunicação infravermelho, presente na maioria destes dispositivos, que não consegue se conectar de forma direta a um *hub* doméstico inteligente (NAZIR, 2019).

Para evitar que *hackers* “roubem” dados dos usuários ou falsifiquem outros aparelhos inteligentes da casa, os pesquisadores recomendam que os usuários comprem lâmpadas que já tenham um *hub* doméstico inteligente. Além disso, o ideal é que as fabricantes melhorem suas medidas de segurança para limitar o acesso das lâmpadas a outros dispositivos da casa.

5.1.2 Falhas permitem acesso de *hackers* a câmeras inteligentes

As câmeras inteligentes modernas contêm muitas funções avançadas, podendo ser utilizadas como monitores infantis sofisticados ou em sistemas de vigilância para identificar invasores quando não há ninguém em casa ou no escritório (SECURITY REPORT, 2018). A Figura 9 mostra exemplo de câmera inteligente fabricada pela empresa sul coreana Hanwha Techwin.

Figura 9 - Câmera Inteligente Multidirecional PNM-9084QZ



Fonte: Hanwha Techwin (2019)

Em pesquisas realizadas no ano de 2018, especialistas da Kaspersky Lab descobriram algo incomum: não apenas uma, mas toda uma série de câmeras inteligentes era vulnerável a vários ataques remotos graves. Isso ocorreu devido ao projeto inseguro no sistema de nuvem e *backbone* das câmeras, inicialmente criado para permitir que os proprietários dessas câmeras acessem ao vídeo de seus dispositivos remotamente. Explorando essas vulnerabilidades, usuários mal-intencionados poderiam executar os seguintes ataques:

- Acessar o fluxo de áudio e vídeo de qualquer câmera conectada ao serviço de nuvem vulnerável;
- Obter acesso remoto à raiz de uma câmera e usá-la como ponto de entrada para ataques sobre outros dispositivos em redes locais e externas;

- Carregar e executar remotamente código malicioso arbitrário nas câmeras;
- Roubar informações pessoais, como as contas dos usuários nas redes sociais e dados pessoais usadas para enviar notificações para os usuários;
- “Travar” câmeras vulneráveis remotamente.

Durante a pesquisa, os especialistas conseguiram identificar quase 2.000 câmeras vulneráveis trabalhando online, mas apenas câmeras que tinham seu próprio endereço IP e, portanto, estavam diretamente disponíveis pela Internet. O número real de dispositivos vulneráveis colocados atrás de roteadores e *firewalls* poderia ser inúmeras vezes maior.

Todos esses ataques eram possíveis porque, segundo as conclusões dos especialistas, a maneira como as câmeras interagem com o serviço de nuvem não é seguro e está aberto a interferências relativamente fáceis. Eles também descobriram que a própria arquitetura do serviço de nuvem é vulnerável a interferências externas (SECURITY REPORT, 2018).

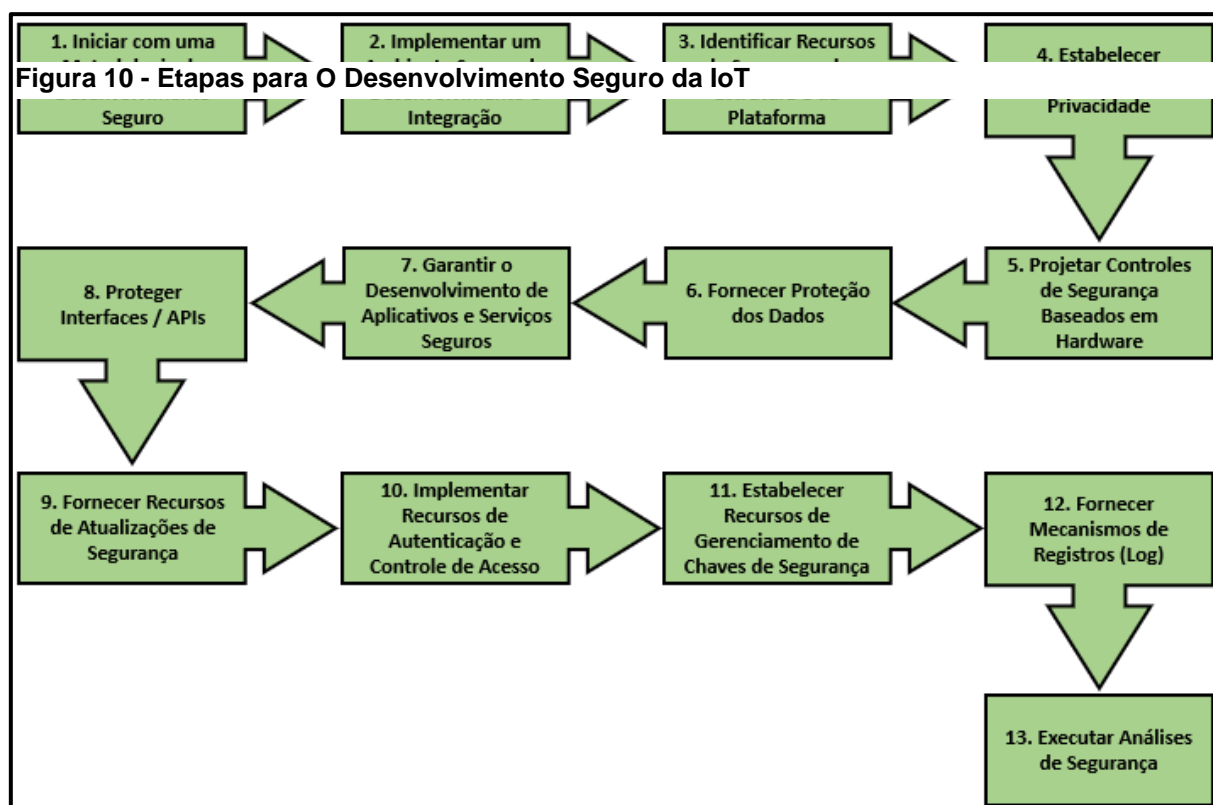
5.1.3 Maior ataque DDoS da história foi causado por *botnet* de dispositivos IoT sequestrados

Uma *botnet* gigante composta de dispositivos conectados à internet sequestrados, como câmeras, lâmpadas e termostatos realizou o maior ataque DDoS de que se tem notícia, contra o blogue Krebs on Security, escrito por Brian Krebs e tido como um dos mais seguros. Foi um ataque tão grande que a Akamai, empresa de tecnologia responsável pela proteção do blogue, após três dias tentando combatê-lo, teve que cancelar sua conta já que defendê-la dos ataques estava consumindo muitos recursos e se tornando muito caro. O ataque de 665 Gbps de tráfego foi quase o dobro de qualquer outro já registrado pela Akamai (NETWORK WORLD, 2016).

5.2 Guia para o Desenvolvimento de Dispositivos IoT Seguros

Este tópico irá fornecer considerações e orientações para projetar e desenvolver dispositivos IoT com um nível razoável de segurança e foi elaborado com base na documentação da CSA (Cloud Security Alliance), organização sem fins lucrativos com foco em segurança em *Cloud Computing* (Computação em Nuvem). É importante notar que estas orientações não substituem as metodologias e técnicas fundamentais de segurança da informação, mas tem o objetivo de mitigar alguns dos problemas mais comuns que podem ser encontrados no desenvolvimento de dispositivos IoT.

Na Figura 13 estão as etapas que devem ser consideradas para o desenvolvimento de dispositivos IoT mais seguros, as quais serão detalhadas



posteriormente.

5.2.1 Iniciar com uma metodologia de desenvolvimento seguro

Atualmente, a maioria das equipes de desenvolvimento de software não estão concentradas suficientemente na segurança da arquitetura, projeto e base de código dos softwares (CSA, 2016). Para enfrentar esse desafio, é necessário recorrer a uma abordagem de engenharia segura, também conhecida como metodologia de desenvolvimento seguro, na qual são apresentadas necessidades além de apenas verificações tecnológicas, devendo ser incluídos ao projeto uma documentação, revisão por pares e incorporação de requisitos de segurança no ciclo de vida do produto.

Na metodologia de desenvolvimento seguro, três itens são abordados (SHOSTACK, 2014), os quais são descritos a seguir:

- **Modelagem de Ameaças:** Como parte do processo de desenvolvimento seguro, a Modelagem de Ameaças deve ser conduzida no software ou hardware a fim de identificar as possíveis ameaças, possibilitando a implementação de controles adequados para atenuar as vulnerabilidades identificadas. Para ajudar os desenvolvedores, estão disponíveis um conjunto de referência a ameaças e problemas dos quais pode-se citar os modelos **Microsoft Threat Modeling**, **OWASP Application Threat Modeling** e o **IEEE Cybersecurity Secure Design**.
- **Avaliação do Impacto na Segurança:** Um diferencial único da IoT é a mistura do mundo físico com o eletrônico. Isso significa que invadir um dispositivo ou serviço IoT pode causar uma reação física. Em dispositivos IoT maiores (por exemplo, carros conectados), é óbvio o impacto potencial causado por um evento malicioso. No entanto, comprometimentos de dispositivos menores, também podem resultar em danos ou prejuízos consideráveis (por exemplo, fechaduras de portas domésticas inteligentes). Os desenvolvedores devem levar isso em

conta e realizar uma avaliação do impacto na segurança como parte do processo de desenvolvimento do software ou hardware.

- **Requisitos e Processos de Segurança:** Uma metodologia de desenvolvimento seguro deve se concentrar em mais do que apenas desenvolvimento. Os desenvolvedores também devem assumir a responsabilidade de criar processos seguros em seus produtos. O BSIMM (Building Security In Maturity Model) permite que as organizações comparem as melhores práticas de desenvolvimento existentes com as usadas em muitas organizações diferentes. O BSIMM consiste em quatro domínios e 12 práticas. A aplicação de cada uma

Domínios BSIMM	Práticas	Aplicações na IoT
Governança	1. Estratégia e Métricas 2. Conformidade e Política 3. Treinamento	<ul style="list-style-type: none"> • Estabelecer uma estratégia e um plano para medir seus controles de segurança contra os padrões da indústria; • Identificar as organizações de testes e consultorias com organizações de testes e consultorias; • Identificar os regulamentos e leis que o dispositivo deve cumprir em um ambiente operacional e acompanhar seu cumprimento; • Treinar todos os membros da equipe em funções relacionadas à proteção de dispositivos IoT e em padrões de ataque típicos para dispositivos IoT vulneráveis.
Inteligência	4. Modelos de Ataque 5. Recursos e Projetos de Segurança 6. Padrões e Requisitos	<ul style="list-style-type: none"> • Pesquisar e executar testes para determinar os recursos de segurança ideais; • Pesquisar maneiras pelas quais produtos similares foram comprometidos e levar em consideração as lições aprendidas; • Construir modelos de ataque, padrões e arquitetura de referência, etc.
SSDL Touchpoints	7. Análise de Arquitetura 8. Revisão de Código 9. Testes de Segurança	<ul style="list-style-type: none"> • Projetar recursos de segurança em camadas que incorporem a segurança eletrônica e física, conforme a necessidade e suportem a confidencialidade, integridade e disponibilidade dos serviços dos dispositivos IoT; • Mitigar e reduzir as superfícies de ataques dos dispositivos IoT o máximo possível; • Projetar serviços associados, adequando à grandes quantidades de dispositivos, de forma segura; • Avaliar o software e hardware durante os testes de segurança.
Implantação	10. Testes de Penetração 11. Ambiente de Software 12. Gerenciamento de configuração e Gerenciamento de Vulnerabilidade	<ul style="list-style-type: none"> • Realizar testes de penetração em um ambiente operacional relevante, para identificar possíveis pontos fracos; • Estabelecer processos para o gerenciamento eficaz das configurações dos dispositivos IoT.

dessas práticas à IoT é descrita na Tabela 3.

Fonte: Adaptado de CSA (2016)

5.2.2 Implementar um ambiente seguro de desenvolvimento e integração

O principal objetivo que um desenvolvedor de produtos IoT de ter é evitar resultados indefinidos, pois isso pode potencialmente se tornam críticos ao lidar com produtos na categoria Cyber Physical Systems (CPS). Uma maneira de se fazer isso, é utilizar padrões seguros de desenvolvimento de *softwares* (CSA, 2016).

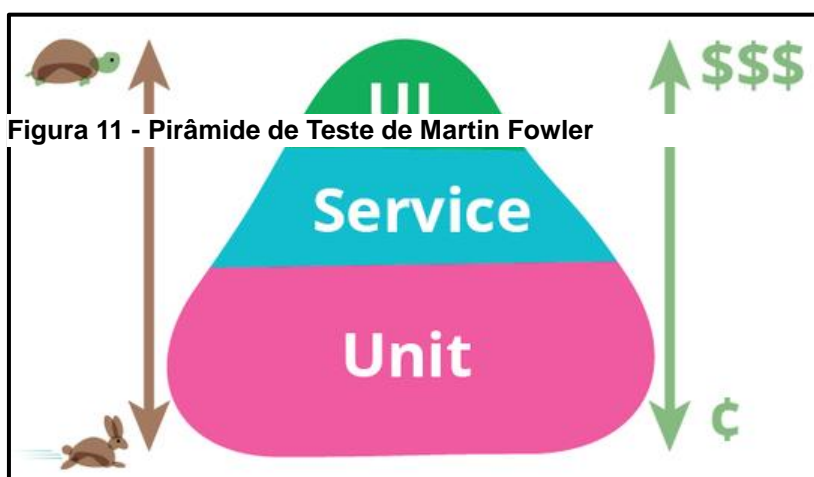
Um ótimo exemplo de padrão seguro, é o desenvolvido pela MISRA (Motor Industry Software Reliability Association) para C e C ++. O MISRA foi projetado para sistemas críticos de segurança e incorpora itens como processo de desenvolvimento de software, treinamento, estilos de codificação, seleção de ferramentas, metodologia de teste e procedimentos de verificação e pode servir de base para o desenvolvimento seguro para IoT (EE TIMES, 2012).

Sendo assim é sugerido que antes de iniciar o desenvolvimento de um produto IoT, quatro itens sejam avaliados, sedo eles:

- **Linguagens de programação:** Avaliar a linguagem de programação que melhor se adeque ao projeto, levando em consideração os recursos de segurança disponíveis. Muitas vezes, os desenvolvedores de produtos IoT também são responsáveis pelo desenvolvimento de aplicativos para smartphones que interagem com o dispositivo e dos serviços em nuvem que coletam informações dos dispositivos. As orientações de segurança apropriadas para a linguagem de programação escolhida, também devem ser revisadas nesse sentido (INFORMATIONWEEK, 2015).
- **Ambientes de desenvolvimento integrado:** No projeto de um dispositivo IoT, os desenvolvedores geralmente precisam escolher um microcontrolado para integrar ao produto, um sistema operacional e softwares com os recursos desejáveis. Sendo assim, é necessário utilizar um processo metódico para o desenvolvimento, integração, teste

e implantação desses recursos, e a segurança deve ser considerada durante cada estágio do ciclo de desenvolvimento.

- **Plugins e Ferramentas de Testes de Segurança:** Plugins como o ZAP (Zed Attack Proxy), criado pela OWASP, podem ser utilizados para ajudar a encontrar vulnerabilidades no código dos softwares. O ZAP é um Scanner de segurança de aplicações web de código aberto, que permite que o código seja verificado dinamicamente e automaticamente, logo após as etapas de compilação serem concluídas. Existem muitas estruturas de teste, políticas de varredura e configurações de sequência disponíveis ao usar o ZAP, que podem ser usadas para melhor integração no ciclo de vida de desenvolvimento do software (OWASP, 2018). É sempre recomendável oferecer suporte à verificação automatizada com teste manual para garantir que as vulnerabilidades de segurança tenham sido consideradas.
- **Testes e Qualidade do Código:** Uma parte importante no desenvolvimento do software são os testes para verificar falhas e vulnerabilidades de segurança no código. A escolha da ferramenta deve ser feita com base na arquitetura em que o produto se encontra. A Pirâmide de Teste de Martin Fowler é uma abordagem ideal para realizar



estes testes (FOWLER, 2012). A Figura 11 ilustra o funcionamento desta pirâmide e logo em seguida é explicado a funcionalidade de cada item:

Fonte: Fowler (2012)

Na base da pirâmide estão os testes unitários (Unit Test), que são a menor parte testável do sistema, possibilitando validar cada parte ou funcionalidade individualmente, no centro da pirâmide estão os testes de serviço (Service Test) onde é testado o funcionamento em conjunto de todos os módulos do sistema, e por fim, no topo está o teste de aceitação (UI Test) onde todo o conjunto de módulos do sistema é testado já com a interface gráfica. A lógica desta abordagem é que os testes da base sejam os realizados em maior frequência, já que são mais rápidos e mais baratos, seguidos dos testes de serviço e por fim o teste de aceitação que é o mais demorado e custoso de se realizar.

Outra parte importante do ambiente de desenvolvimento seguro é a necessidade de painéis de qualidade de código pois os dispositivos IoT devem ser suportados por relatórios que forneçam informações sobre a qualidade do software. Estes painéis possibilitam revisar o progresso dos testes, construir estados, avançar na resolução e fechamento de *bugs*, taxa de reativações de *bugs*, porcentagem de código que foi testado e as tendências nas alterações do código.

5.2.3 Identificar recursos de segurança da estrutura e da plataforma

As estruturas oferecem a capacidade de desenvolver dispositivos interoperáveis, por isso é importante decidir se será criado um dispositivo independente ou se será utilizada uma estrutura já disponível (CSA, 2016).

As estruturas de integração são úteis no desenvolvimento de dispositivos IoT que devem se comunicar com outros dispositivos para realizar trabalhos automatizados. Os desafios associados a fazer com que todos trabalhem juntos com segurança se tornam evidentes, principalmente quando são fabricados por diferentes empresas. As estruturas de integração fornecem as ferramentas necessárias para que os dispositivos operem no mesmo ecossistema, mesmo sendo fabricados por empresas distintas (UVIASE; KOTONYA, 2018).

Do ponto de vista da segurança, é importante selecionar uma estrutura que forneça aos desenvolvedores as ferramentas necessárias para implementar essa

interoperabilidade com segurança. Isso começa com o conceito de integração segura e se estende à capacidade de oferecer suporte ao gerenciamento proativo do dispositivo e às comunicações seguras.

Na escolha de uma estrutura segura e adequada ao projeto, os seguintes itens devem ser avaliados (CSA, 2016):

- **Integração do dispositivo:** Este é o processo para conectar o dispositivo a uma rede específica. Deve possibilitar o uso de credenciais de rede e permitir a mudança de propriedade posteriormente;
- **Configuração:** Inclui a capacidade de nomear / renomear um dispositivo IoT, definir senhas ou redefinir o dispositivo;
- **Gerenciamento de Ativos:** isso inclui manter o conhecimento da localização de um dispositivo, seu perfil de *hardware* / *software*, bem como a capacidade de manter atualizações de *firmware* / *software*;
- **Descoberta:** Este é o processo para permitir a descoberta de outros dispositivos e serviços;
- **Conexões seguras:** Isso inclui os protocolos e algoritmos necessários para dar suporte à autenticação do dispositivo em outros dispositivos / serviços; verificação de credenciais de autenticação de servidor / dispositivo ponto a ponto e criptografia de comunicações. Isso pode incluir a instanciação de protocolos como TLS e DTLS. Algoritmos criptográficos suficientemente fortes também devem ser disponibilizados.
- **Gateways na nuvem:** Os *gateways* nem sempre precisam ser dispositivos fisicamente separados, embora possam assumir esse formato. Esses *gateways* fornecem um link entre uma rede local e a nuvem para suportar interações globais. Os *gateways* devem

implementar APIs seguras nos provedores de serviço em nuvem com criptografia, autenticação e integridade aplicadas.

5.2.4 Estabelecer proteções de privacidade

A compreensão dos riscos referentes a exposição de dados sensíveis que um dispositivo IoT pode oferecer, é uma questão crítica e as fabricantes de dispositivos têm a responsabilidade de entender os tipos de dados que serão processados ou armazenados nos dispositivos, bem como os dados que são transmitidos aos serviços e aplicativos móveis conectados aos dispositivos (CSA, 2016). Esse entendimento fornece a base para o desenvolvimento de controles de segurança que permitem às organizações proteger seus ativos de informações (ANDREA; CHRYSOSTOMOU; HADJICHRISTOFI, 2015). A seguir estão algumas orientações para proteção da privacidade que devem ser consideradas no desenvolvimento de um dispositivo IoT:

- **Projetar dispositivos, serviços e sistemas de IoT para coletar apenas a quantidade mínima necessária de dados:** os sensores podem vaziar indevidamente informações sobre alguém que interage com o dispositivo, sendo assim é importante que seja reduzido ao mínimo possível a quantidade de dados coletados e que se ofereça suporte ao anonimato, quando possível.
- **Analisar a finalidade de uso do dispositivo e oferecer o suporte necessário para atender os requisitos da legislação:** Ao trabalhar com sistemas IoT, a importância em atender os requisitos regulatórios de normas e legislações, provavelmente aumentará. Esse é um fator-chave, por exemplo, para dispositivos relacionados à saúde, pois esses dispositivos podem não apenas fazer a contagem de calorias ou monitorar os níveis de condicionamento físico, mas também podem ler informações mais sensíveis sobre as condições de saúde do usuário. Outros desafios de conformidade podem surgir para os dispositivos projetados para serem usados por crianças. Nesses casos, é necessário que os dispositivos sejam compatíveis com a legislação de proteção de dados pessoais de cada país.

- **Desenvolver termos aceitação de uso para dispositivos, serviços e recursos do sistema:** Mesmo que o dispositivo não ofereça uma interface gráfica, é necessário que os desenvolvedores pensem em métodos para permitir que o usuário conheça e tenha a opção para autorizar ou não a coleta e compartilhamento de suas informações privadas, de forma clara e objetiva. Fornecer essas opções de aceitação em dispositivos que fazem interface com o dispositivo IoT, por exemplo, smartphones, seria a escolha lógica para o mercado consumidor, já para dispositivos IoT voltados para uso comercial, uma opção a ser considerada pelos desenvolvedores, é o fornecimento de folhas de especificações descrevendo todos os dados que serão coletados pelo dispositivo IoT.

5.2.5 Projetar controles de segurança em *hardware*

Vulnerabilidades e configurações incorretas de *software* não são o único vetor de ataque com o qual os desenvolvedores de dispositivos IoT devem se preocupar. Também é necessário realizar a proteção do *hardware* para evitar que invasores possam acessar, extrair e modificar o *firmware* do dispositivo (CSA, 2016). Sendo assim, alguns elementos devem ser considerados durante o desenvolvimento do projeto:

- **Microcontrolador:** A seleção da base SoC (System On Chip) que será utilizada no desenvolvimento do dispositivo IoT é crucial para a implementar a segurança. É importante que o SoC escolhido ofereça suporte à 6 elementos (TOBERGTE; CURTIS, 2013), sendo eles 1) Gerenciador de inicialização (*bootloader*) com suporte a criptografia (possibilita atualizações seguras de *firmware*); 2) Acelerador de hardware criptográfico (possibilita o processamento eficiente de algoritmos de criptografia); 3) Proteção da memória segura; 4) Proteção incorporada contra adulterações; 5) Proteção contra engenharia reversa; 6) Mecanismos seguros para armazenamento de chave criptográfica na memória não volátil.

- **Módulos de Plataforma Confiáveis (TPM):** As proteções de segurança de hardware são realizadas através de módulos de segurança. O TPM (Trusted Platform Module) possibilita realizar transmissões de dados criptografados através de autenticação e autorização, utilizando padrões conhecidos de criptografia. Embora esse recurso tenha aplicação limitada em dispositivos IoT, devido a restrições de hardware e também questões de custo, é recomendado utilizar esta opção ao criar um dispositivo que processe ou armazene informações confidenciais (ELECTRONICS 360, 2015).
- **Unidades de Proteção de Memória (MPUs):** As MPUs (Memory Protection Units) fornecem regras de acesso aos locais de memória. Dispositivos IoT que incorporam uma MPU podem controlar qual memória pode ser lida, gravada e executada.
- **Módulos de Criptografia:** É importante identificar os limites de segurança que exigem uma maior atenção e proteção extra. A identificação das proteções criptográficas físicas do dispositivo fornecem uma visão das áreas do *hardware* e do *software* que devem receber o grau mais significativo de proteções. Dentro do limite criptográfico, deve-se encontrar funções como processamento criptográfico e gerenciamento de chaves que oferecem proteções de segurança adicionais contra a exposição da chave criptográfica e outros parâmetros de segurança sensíveis. Os desenvolvedores de IoT podem adquirir módulos validados ou criar seus próprios módulos (ELECTRONICS 360, 2015).
- **Proteções Físicas do Dispositivo:** Deve-se considerar a aplicação de proteções de segurança física nos dispositivos IoT, como a detecção de violação do equipamento e até a “zeroização” (exclusão de parâmetros sensíveis), em casos extremos. As proteções contra adulteração evitam o comprometimento de informações confidenciais armazenadas no dispositivo IoT. Pode ser implementada de maneira a alertar a uma tentativa de comprometimento físico do dispositivo, ou realizar a

proteção de forma ativa. O *hardware* pode responder com várias contramedidas, desde a redefinição do sistema até a exclusão de informações críticas, como códigos ou senhas.

- **Autoteste:** Implemente autotestes na inicialização para verificar os recursos de segurança do dispositivo. Após a identificação de um erro, o mesmo deve ser registrado e se possível o processamento deve ser interrompido.
- **Interfaces Físicas Seguras:** Um dos objetivos associados à proteção de interfaces físicas é proteger contra o descarregamento do *firmware* do produto para análise e modificação. A maioria dos dispositivos IoT não possui proteção contra adulteração incorporada ao esquema de proteção física, possibilitando que invasores se conectem através de interfaces como JTAG (Joint Test Action Group), UART (Universal Asynchronous Receiver Transmitter), e USB (Universal Serial Bus). Portanto, é importante incluir uma etapa no processo de engenharia que desabilite as interfaces antes do envio do dispositivo e quando possível bloquear as portas USBs permitindo que realizem apenas conexão com dispositivos confiáveis. Além disso, restrições de senha podem ser colocadas nas interfaces.

5.2.6 Fornecer proteção dos dados

Um dos pontos importantes a serem observados sobre a IoT é que a Internet tradicional, como é conhecida hoje, está concentrada na comunicação de humanos para máquinas. No entanto, com a rápida adoção e evolução da IoT, será necessário incluir transações de máquina para máquina e isso significaria mais uma diferença crítica pois não haverá um fluxo constante de dados, e sim um fluxo em rajadas de dados, dada a natureza e o uso desses dispositivos (HUREL; LOBATO, 2018). Também é importante ressaltar que os pacotes de dados terão tamanho reduzido e serão muito direcionados e o processamento em tempo real ocorrerá em um *gateway* ou na nuvem (CSA, 2016).

Dado este contexto, é importante a escolha do conjunto de protocolos apropriados ao tipo de dado que está sendo processado, levando em consideração a tolerância a falhas de comunicação que podem ocorrer (HUREL; LOBATO, 2018). Uma das principais considerações de segurança que devem ser examinadas para qualquer protocolo é o processo de ingresso ou emparelhamento. Por exemplo, quando um dispositivo ingressa em uma rede existente, quais controles são implementados para garantir que apenas um dispositivo legítimo possa ingressar na rede?

Há muitas opções para escolher e a escolha do protocolo de comunicação dependerá da finalidade de uso do dispositivo IoT. No entanto o padrão 802.15.4 pode ser usado como base para outros protocolos de IoT, como o *ZigBee*.

A Tabela 4 fornece informação dos principais protocolos de comunicação que podem ser utilizados nos dispositivos IoT, bem como os aspectos de segurança que devem ser considerados para cada um deles.

Tabela 4 - Protocolos para Dispositivos IoT

Protocolo de comunicação IoT	Aspectos de Segurança
LTE	Utiliza o protocolo AKA (Authentication and Key Agreement) como base para autenticação entre o dispositivo IoT e a rede principal.
GPRS	Todos os dados e sinais são criptografados usando o algoritmo GEA (GPRS Encryption Algorithm). Usa um cartão SIM para armazenar identidades / chaves
GSM	Tecnologia Celular, baseado no acesso múltiplo por divisão de tempo (TDMA). Os dispositivos IoT são equipados com cartões SIM para armazenar a identidade / chave de autenticação. Os possíveis problemas que podem surgir incluem a inserção de estações base maliciosas, chaves fracas (quantidade pequena de bits) e transmissão de chaves em texto não criptografado pela rede.
UMTS	O sinal e os dados do usuário são criptografados. Utiliza chave criptográfica de 128 bits e o algoritmo KASUMI com dois modos: criptografia e proteção de integridade de dados.
CDMA	Tecnologia celular, CDMA (Code Division Multiple Access). Nenhum cartão SIM é utilizado.
LoRaWAN (Long Range Wide Area Network)	Taxas de dados suportadas entre 0,3 kbps e 50 kbps. Depende do uso de três chaves: <ul style="list-style-type: none"> • Chave de rede exclusiva • Chave de aplicativo exclusiva para segurança de ponta a ponta na camada de aplicativo • Chave específica do dispositivo
802.11	O WiFi existe há muito tempo. Considerar que os dispositivos precisarão ser provisionados com as chaves que lhes dão acesso a uma rede WiFi.
802.15.4	Permite que protocolos de camada superior definam os controles de autenticação / criptografia / integridade.
6LoWPA (IPv6 over Low power Wireless Personal Area Networks)	Uma rede sem fio de baixa potência projetada para oferecer suporte à junção automática de dispositivos à rede sempre que possível. Requer a introdução de um servidor de inicialização LoWPAN para provisionar informações de inicialização para dispositivos 6LoPAN.
ZigBee	O ZigBee utiliza o padrão IEEE 802.15.4 para implementar as camadas MAC (Medium Access Control) e PHY (Physical Layer), fornecendo suporte às topologias estrela, árvore e malha. Existe um pouco fraco durante a conexão inicial de um dispositivo que não foi pré-configurado à rede, pois durante esta conexão, uma única chave sem proteção pode ser enviada, causando uma vulnerabilidade que pode resultar na obtenção da chave por qualquer dispositivo de escuta.
Zwave	O ZWave é uma rede em malha que utiliza ondas de rádio de baixa energia para se comunicar de um dispositivo para outro. Utiliza chaves de criptografia e chaves de autenticação dos dados de origem. Essas chaves são enviadas de forma protegida.
Thread	Desenvolvido com base no padrão 802.15.4, suporta conexão de até 250 dispositivos em uma rede e também oferece suporte a criptografia AES. Utiliza o protocolo PAKE (Password Authenticated Key Exchange) e a camada MAC 802.15.4 utiliza uma chave de rede.
Sigfox	Utiliza o sistema de comunicação UNB (Ultra Narrow Band) na faixa de 915 MHz (EUA) e 868 MHz (Europa) e chaves privadas para assinatura de mensagens. Possui um limite de 140 mensagens que podem ser enviadas por dia em cada dispositivo e estabelece proteções anti-repetição.
Bluetooth / Bluetooth-LE	A versão 4 da especificação adicionou a o método de criptografia de curvas elípticas ECDH (Elliptic Curve Diffie Hellman) para troca de chaves durante o processo de emparelhamento. O Bluetooth-LE usa uma chave simétrica de 128 bits para proteção de confidencialidade.
NFC	Possui proteção de segurança limitada e é frequentemente utilizada em conjunto a protocolos.
Wave 1609	Predominante na comunicação com veículos conectados. Depende muito do padrão IEEE 1609.2, que oferecem suporte à marcação de atributos.

Fonte: Adaptado de CSA (2016)

5.2.7 Garantir o desenvolvimento de aplicativos e serviços seguros

Os dispositivos IoT operam como parte de um ecossistema maior, onde cada ponto de integração pode representar uma via potencial para uma possível invasão (CSA, 2016). É necessário garantir que os aplicativos que irão interagir com esses dispositivos tenham sido desenvolvidos utilizando as práticas recomendadas de desenvolvimento seguro (MICROSOFT, 2018). A seguir estão algumas recomendações que podem ser utilizadas no desenvolvimento de aplicativos móveis e serviços para dispositivos IoT:

- Os desenvolvedores de aplicativos para smartphones devem usar credenciais de segurança para permitir comunicações autenticadas protegendo a integridade dos dispositivos IoT;
- Em alguns casos, os desenvolvedores devem considerar a implementação de certificados fixos para impedir que ataques MITM ocorram em redes não confiáveis;
- Os desenvolvedores de produtos de IoT também devem considerar limitações nos privilégios concedidos aos aplicativos móveis, limitando o escopo de capacidade que um aplicativo móvel pode exercer sobre qualquer dispositivo IoT específico. Por exemplo, um aplicativo que controla a funcionalidade em um veículo conectado à Internet não deve afetar os controles que não devem ser explicitamente administrados remotamente.
- Os recursos de acesso privilegiado precisam ser considerados para a configuração do dispositivo IoT e para os aplicativos que interagem com eles;
- Os dispositivos IoT geralmente fazem interface com serviços em nuvem com o objetivo de melhorar a coleta, análise e processamento de dados entre os componentes da IoT. Assim como os aplicativos móveis, os desenvolvedores de serviços em nuvem devem usar rigor na proteção

de seus sistemas aproveitando os processos e estruturas de padrões para proteger serviços internos e de terceiros.

5.2.8 Proteger interfaces / APIs

Uma das considerações mais importantes ao desenvolver produtos de IoT é a segurança da interface, também conhecida como API (CSA, 2016). Existem muitos serviços em nuvem com os quais os dispositivos IoT podem interagir, além de aplicativos para smartphones, e a API pode expor os provedores de serviços a ataques de negação de serviço quando não são adequadamente protegidas (RED HAT, 2019). A seguir são apresentadas algumas recomendações para melhor proteger estas interfaces:

- Usar técnicas como limitação da taxa de tráfego protege contra dispositivos IoT comprometidos que tentam sobrecarregar o serviço com solicitações.
- Os *gateways* devem verificar o formato adequado das mensagens, garantindo que apenas os tipos de dados permitidos serão transmitidos. Isso diminui o potencial de inserção de códigos maliciosos nas comunicações da API que podem resultar no comprometimento de um serviço de nuvem da IoT.
- O tratamento de erros também deve ser considerado. Deve-se evitar fornecer respostas muito detalhadas pois apesar de contribuir para a solução de problemas, pode fornecer ao invasor informações significativas que podem potencializar seu ataque.
- Utilizar a técnica de marcas temporais (timestamps), com data e hora e / ou contadores, nas estruturas das mensagens, a fim de proteger contra ataques do tipo repetição.
- Sempre que possível, implementar controles de autenticação e autorização robustos, limitando a exposição das chaves da API.

- Utilizar protocolos como TLS e DTLS para criptografar as comunicações da API e também utilizar certificados fixos para proteger a transmissão de informações confidenciais.

5.2.9 Fornecer recursos de atualizações de segurança

Determinar a estratégia para atualizar o *firmware* e o *software* do dispositivo IoT é um dos principais desafios do projeto (PAUL, 2019), pois a falta de segurança durante o processo de atualizações possibilita que um indivíduo mal-intencionado tenha acesso ao *firmware* legítimo e o substitua por um *firmware* modificado o qual pode desativar os controles de segurança e implementar novos recursos, ou fornecer um mecanismo para a extração de dados (CSA, 2016). Algumas considerações devem ser observadas na implementação das atualizações de segurança:

- Determinar se as atualizações deverão ocorrer de forma ativo/passivo ou ativo/ativo. É possível corrigir e trocar em tempo real por um componente corrigido. O *software* ou *firmware* pode ser isolado em caixas de proteção para validar a segurança antes da implementação.
- O *firmware* deve ser protegido de ponta a ponta e todo o ciclo de vida deve ser considerado. O carregamento inicial do *firmware* deve ocorrer em uma instalação segura, usando processos seguros.
- Deve-se criar um processo de contingência no caso de uma sessão de atualização ser interrompida, possibilitando reverter para a versão anterior, evitando a interrupção do dispositivo IoT quando a atualização for malsucedida.
- É importante entender quais permissões precisam estar associadas ao processo de atualização e definir quem será responsável por realizar esta atualização, as quais podem ser realizadas pelo proprietário do dispositivo ou automaticamente pela infraestrutura de IoT. Muitas vezes, as atualizações automáticas são mais eficientes pois são realizadas de formas mais rápida, No entanto, deve-se considerar também se um

invasor pode usar o processo de atualização para executar um ataque do tipo DoS no dispositivo.

- Em relação à autenticação do processo de atualização, é necessário entender que a autenticação do *firmware* deve ser de ponta a ponta. Isso requer que o dispositivo tenha armazenamento seguro para uma raiz confiável, que possa ser usada para validar uma assinatura aplicada ao *firmware* na infraestrutura.
- proteger o dispositivo contra gravação para evitar modificações não autorizadas de *firmware*.

5.2.10 Implementar recursos de autenticação e controle de acesso

Os dispositivos IoT devem conter recursos de proteção de credenciais, evitando que senhas, tokens de acesso ou chaves privadas sejam “roubados” (CASTRO; MACEDO; DOS SANTOS, 2018). Isso significa que os desenvolvedores devem trabalhar em maneiras de implementar o armazenamento seguro, além de impedir que essas credenciais vazem caso o dispositivo “trave” e a memória seja explorada (CSA, 2016). Este tópico irá apresentar algumas recomendações que podem ser utilizadas para prover os recursos de proteção e armazenamento seguro de credenciais nos dispositivos IoT.

- **Autenticação:** Um dos desafios associados à autenticação e autorização na IoT é a gama de dispositivos envolvidos para o usuário final e independentemente da quantidade, solicitar aos usuários que configurem manualmente cada dispositivo não é uma boa proposta. A introdução da comunicação entre os dispositivos pode tornar essa questão ainda mais complexa, pois muitos dispositivos que eventualmente trabalharão em conjunto pertencerão a diferentes fabricantes e até funcionaram em estruturas diferentes. Felizmente, muitos dos protocolos de IoT que oferecem suporte à comunicação entre dispositivos vêm com a capacidade de configurar conexões seguras. A

Tabela 5 fornece uma visão das opções de configuração disponíveis para alguns desses protocolos.

Tabela 5 - Protocolos para Autenticação M2M

Protocolo	Opções de Autenticação M2M	Aspectos
MQTT (Message Queuing Telemetry Transport)	Usuário / Senha	O MQTT permite o envio de um nome de usuário e senha, embora recomende que a senha não tenha mais de 12 caracteres. Nome de usuário e senha são enviados de forma clara e, como tal, é essencial que o TLS seja empregado ao usar o MQTT.
CoAP (Constrained Application Protocol)	Chave Pré-Compartilhada Chave Pública Bruta Certificado	O CoAP suporta várias opções de autenticação para comunicação entre dispositivos. Pode ser utilizado em conjunto com o protocolo D-TLS (Datagram TLS) para serviços de confidencialidade de nível superior.
XMPP (Extensible Messaging and Presence Protocol)	Várias opções disponíveis, dependendo do protocolo	O XMPP suporta uma variedade de padrões de autenticação por meio dos mecanismos SASL - RFC4422 (Simple Authentication and Security Layer). incluem autenticação unidirecional anônima e mútua com senhas criptografadas, certificados e outros meios implementados através da camada de abstração SASL.
DDS (Data Distribution Service)	Tokens de certificados X.509 (PKI)	Fornecer autenticação de terminal e estabelecimento de chave para executar a autenticação de origem de dados da mensagem subsequente. Ambos os certificados digitais e vários tipos de token de identidade / autorização são suportados.
HTTP / REST (Hypertext Transfer Protocol) / (Representational State Transfer)	Autenticação básica (texto não criptografado) (métodos TLS) OAUTH2	HTTP / REST normalmente requer o suporte do protocolo TLS para serviços de autenticação e de confidencialidade. Embora a autenticação básica (onde as credenciais são passadas de forma clara) possa ser usada sob a cobertura do TLS, essa não é uma prática recomendada. Em vez disso, pode-se defender uma abordagem de autenticação baseada em token, como OAUTH2

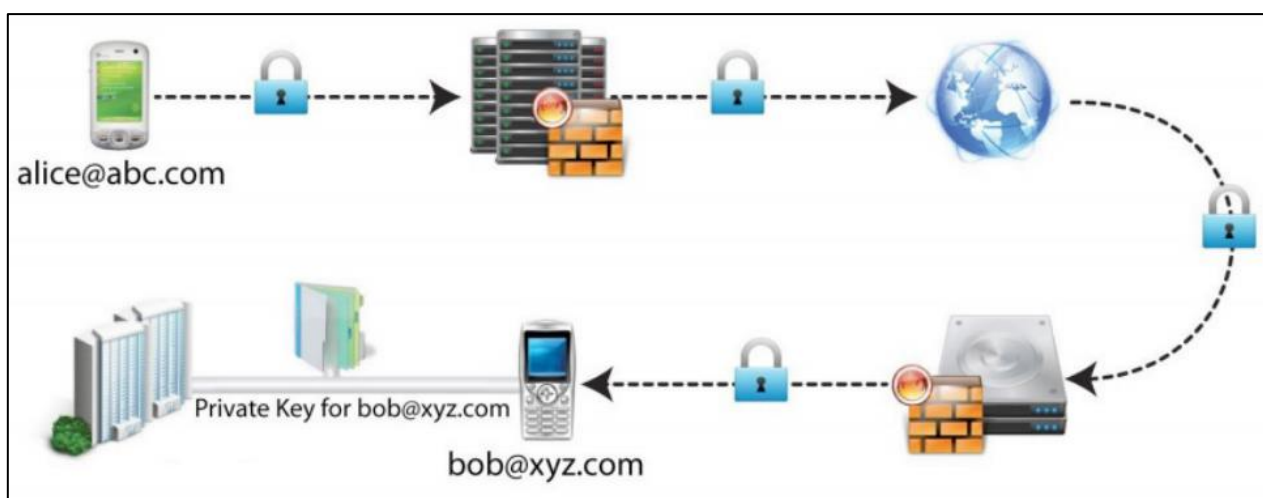
Fonte: Adaptado de CSA (2016)

- Certificado de autenticação:** Um certificado está vinculado a um par de chaves criptográficas (público / privado). A chave pública geralmente é incorporada diretamente no certificado e é disponibilizada para qualquer pessoa que precise validar a autenticidade da transação. A chave privada é protegida e, no caso da autenticação, é usada para assinar digitalmente um objeto. Uma validação ocorre quando a chave pública

associada é usada para validar a assinatura aplicado ao objeto. Existem protocolos disponíveis para auxiliar esse processo, incluindo o protocolo SCEP (Simple Certificate Enrollment Protocol) e o protocolo EST (Enrollment over Secure Transport).

- **Biometria:** Também pode ser utilizada a biometria como método de identificação em transações de autenticação. Biometria, como impressões digitais ou mesmo impressões de voz, podem ser utilizadas para autenticação.
- **Criptografia de autenticação sem certificado (CLAE):** Um método relativamente novo para fornecer autenticação na IoT é conhecido como CLAE (Certificate-Less Authenticated Encryption) ou Criptografia de Autenticação sem Certificado. O CLAE permite que o remetente de uma mensagem verifique os parâmetros públicos do servidor antes da criptografia da mensagem. Isso permite verificar se os parâmetros públicos usados para criptografar a mensagem não foram violados, em vez de usar certificados emitidos por uma CA (Autoridade de Certificação). A Figura 12 ilustra o funcionamento do CLAE.

Figura 12 - Criptografia de Autenticação Sem Certificado



Fonte: CSA (2016)

- **OAuth 2.0:** O OAuth 2.0 requer um servidor de autorização que verifique a identidade do usuário / dispositivo e emita tokens para acesso. Esse é um mecanismo centralizado e requer que o ambiente em que o dispositivo IoT irá operar, tenha acesso a um servidor de autorização. Isso também significa que o servidor deve estar protegido contra possíveis invasões.
- **Acesso gerenciado pelo usuário (UMA):** UMA (User Managed Access) é um protocolo de gerenciamento de acesso baseado no OAuth com suporte à capacidade das partes de compartilhar e revogar autorizações de informações. Esse compartilhamento pode ser realizado em tempo real. A UMA parece fornecer o maior valor em cenários em que uma pessoa está envolvida na transação entre dispositivos (por exemplo, através do conceito de compartilhamento em tempo real ou, mais importante, da possibilidade de optar por compartilhar (ou não) em tempo real). UMA é um padrão a ser considerado quando a privacidade é altamente importante e o ambiente de compartilhamento é complexo.

5.2.11 Estabelecer recursos de gerenciamento de chaves de segurança

O gerenciamento de chaves é um tópico quase tão importante quanto a criptografia e é frequentemente implementado de maneira insegura. A divulgação não autorizada de chaves criptográficas dificulta o uso da criptografia e pode levar à perda de dados (CSA, 2016). O gerenciamento de chaves, portanto, aborda como as chaves criptográficas são gerenciadas. A Tabela 6 descreve o processo de geração das chaves criptográficas.

Tabela 6 - Processo de Geração de Chaves Criptográficas

Fase	Descrição
Geração da Chave	Como, quando e em quais dispositivos as chaves são geradas
Derivação da Chave	Construindo chaves criptográficas a partir de outras chaves e variáveis
Estabelecimento da Chave Aceitação da Chave Trasmissão da Chave	Cálculo algorítmico de duas partes do material de codificação Encapsulamento seguro e envio de chaves de um dispositivo para outro
Armazenamento da Chave	Armazenamento seguro de chaves (freqüentemente criptografadas usando "chaves de criptografia de chaves") e em que tipo de dispositivo (s)
Vida Útil da Chave	Quanto tempo uma chave deve ser usada antes de ser destruída (zerada)
Descarte da Chave	Destruição segura da chave
Contabilidade	Identificação, rastreamento e contabilização da geração, distribuição e destruição da chave entre as entidades

Fonte: Adaptado de CSA (2016)

Na IoT é importante equilibrar segurança versus desempenho. Isso está relacionado ao tempo de vida estabelecido para chaves criptográficas. Em geral, quanto menor a vida útil da chave, menor será o impacto caso ela seja comprometida, porém, mais frequentemente as chaves precisam ser geradas ou estabelecidas e isso afeta diretamente o desempenho do dispositivo.

O gerenciamento seguro de chaves também exige que os fabricantes conheçam bem a hierarquia de chaves criptográficas, especialmente no processo de fabricação e distribuição de dispositivos. A chave incorporada ao dispositivo pode ser originária do fabricante, nesse caso, o fabricante deve ser rigoroso quanto à proteção dessas chaves.

5.2.12 Fornecer mecanismos de registros

Um aspecto crítico da segurança da informação para uma empresa são os registros (logs) dos eventos que ocorrem em seu ambiente de T.I. Um exemplo disso, é quando os usuários fazem login em dispositivos e serviços e principalmente quando há falhas neste processo (CSA, 2016). Sendo assim, é de extrema importância para o ambiente corporativo que os dispositivos IoT forneçam Logs com informações necessárias, para que a equipe de T.I possa monitorar a segurança.

Muitos dispositivos IoT fornecem algum nível de Log via APIs REST. Embora haja várias maneiras de oferecer suporte à dados de Log, é importante fornecer visibilidade suficiente das ações que ocorrem no dispositivo. Isso inclui no mínimo:

- Solicitações de conexão;
- Autenticações (falha / êxito);
- Tentativas de abuso de privilégio / tentativas de elevação de privilégio;
- Recebimento de mensagens malformadas;
- Atualizações de *firmware* / *software* bem-sucedidas ou com falha;
- Tentativas locais de *login*
- Mudanças na configuração
- Atualizações da conta
- Acesso protegido à memória
- Violação física

5.2.13 Executar análises de segurança

No processo de desenvolvimento de dispositivos IoT, tanto o *software* como o *hardware* devem ser testado e revisado. Abordagens como *Common Criteria* (CC) podem ser utilizada como referência para a criação de recursos de segurança baseados em *hardware* (CSA, 2016).

O projeto OWASP fornece excelentes ferramentas para entender os aspectos de segurança durante o desenvolvimento do *software* e também para a utilização de *feedback loops*, que vinculam projeto, desenvolvimento e teste. A utilização de

feedback loops permitem atualizações do projeto orientadas pela identificação de pontos fracos durante o teste ou implantação.

Existem muitos tipos de testes que podem ser empregados no desenvolvimento de dispositivos IoT e cada um deles desempenha um papel crítico na manutenção da postura de segurança do dispositivo:

- Teste de segurança de aplicativos estáticos (SAST)
- Teste Dinâmico de Segurança de Aplicativos (DAST)
- Teste interativo de segurança de aplicativos (IAST)
- Superfície de ataque e vetores
- Biblioteca de Terceiros
- Fuzzing
- Personalizado por vetor de ameaça

Os desenvolvedores de dispositivos IoT também podem utilizar serviços de terceiros para testar seus dispositivos. Existem diversos serviços disponíveis tanto pagos como gratuitos, entre eles podem ser citados Builditsecure.ly e o Crowdstrike.

O ICSA Labs também desenvolveu um programa confiável para testar dispositivos IoT, o qual foca no teste de seis componentes:

- Comunicações
- Alerta / registro
- Segurança da plataforma
- Criptografia
- Segurança física
- Autenticação

Independente da ferramenta escolhida, o resultado dessas avaliações fornece informações valiosas sobre o comportamento de segurança do dispositivo permitindo tomar as ações necessárias para mitigar os problemas encontrados.

CONSIDERAÇÕES FINAIS

A IoT é uma tecnologia muito promissora, que oferece diversos benefícios como conforto e comodidade para os consumidores domésticos e aumento da produtividade com redução de custos para a indústria.

Porém, como foi constatado, o principal obstáculo na sua implementação está na dificuldade em garantir a segurança das informações presentes nos dispositivos interconectados e isso é de extrema importância, pois sabe-se que tanto as empresas quanto os usuários estão preocupados com a proteção e privacidade de seus dados.

Diante disso, o objetivo geral desta pesquisa foi identificar e analisar os principais problemas relacionados à segurança da informação, que podem surgir com a utilização da tecnologia IoT. Consta-se que este objetivo pôde ser atendido pois conseguiu-se, utilizando como base o estudo de pesquisadores e especialistas da área, detalhar de forma objetiva os problemas presentes nos dispositivos utilizados por esta tecnologia, como pode ser visto no capítulo 4.

O objetivo específico inicial foi identificar as vulnerabilidades, ameaças e tipos de ataque em dispositivos IoT, os quais foram apresentados nos capítulos 4.1 e 4.2.

O segundo objetivo específico foi expor casos notórios de problemas de segurança envolvendo IoT o qual pode ser verificado no capítulo 5.1.

O terceiro objetivo específico foi encontrar possíveis soluções e contramedidas para tornar o ambiente IoT mais seguro, o qual foi atendido no capítulo 4.3 e também no capítulo 5.1, por meio do qual foi apresentado um guia de boas práticas para a implementação da tecnologia IoT.

O trabalho parte da hipótese de que há muitas vulnerabilidades presentes nos dispositivos inteligentes, que são utilizados pela tecnologia IoT, e com base na pesquisa realizada, pode-se afirmar que há um longo caminho a ser trilhado pelas fabricantes de *hardware* e pelos desenvolvedores de *softwares*, pois muitos são os problemas de segurança da informação e privacidade a serem resolvidos.

A pesquisa identificou que os principais problemas encontrados nos dispositivos IoT utilizados atualmente são: limitações no armazenamento; problemas de segurança e privacidade nos dados transmitidos e armazenados; falta de padronização entre as fabricantes e vulnerabilidades na segurança física dos dispositivos.

O principal método empregado na realização deste trabalho foi pesquisas em artigos, livros e documentos técnicos de especialistas, empresas e instituições da área de segurança da informação e IoT. Diante da metodologia utilizada, percebe-se que o trabalho poderia incluir testes práticos a fim de exemplificar, e explorar melhor as vulnerabilidades e possível correções. Porém, devido a limitação de tempo e conhecimentos necessários, isso não foi possível de ser realizado.

Como recomendação para trabalhos futuros, propõe-se a implementação de simulações que visem a mitigação de ataques conhecidos. Um estudo sobre métodos utilizados para diminuir e até mesmo extinguir os efeitos causados por ataques nas redes de IoT, juntamente com simulações que comprovem a eficácia dos códigos implementados para a mitigação de cada ataque.

REFERÊNCIAS

ANDREA, I.; CHRYSOSTOMOU, C.; HADJICHRISTOFI, G. **Internet of Things: Security Vulnerabilities and Challenges**, IEEE, 2015. Disponível em: https://www.researchgate.net/profile/George_Hadjichristofi/publication/304408245_Internet_of_Things_Security_vulnerabilities_and_challenges/links/598188270f7e9b7b524b92ac/Internet-of-Things-Security-vulnerabilities-and-challenges.pdf. Acesso em: 01 out. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Rio de Janeiro: ABNT, 2005. Disponível em: http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf. Acesso em: 16 set. 2019.

ASTHON, K. That “Internet of Things” Thing. **RFID Journal**, Melville, p. 1, 2009. Disponível em: <http://www.rfidjournal.com/article/print/4986>. Acesso em: 17 set. 2019.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2005.

CARRION, P.; QUARESMA, M. Internet da Coisas (IoT): Definições e aplicabilidade aos usuários finais. **Human Factors in Design**, Florianópolis, v. 8, n. 15, p. 49–66, 2019. Disponível em: <http://www.revistas.udesc.br/index.php/hfd/article/view/2316796308152019049>. Acesso em: 11 set. 2019.

CASTRO, T. O.; MACEDO, D. F.; DOS SANTOS, A. L. **Controle de Acesso IoT Escalável e ciente de contexto suportando múltiplos usuários**, 2018. UFMG, Belo Horizonte, 2018. Disponível em: http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/09-181304_1.pdf. Acesso em: 18 nov. 2019.

CERT.BR. **Cartilha de Segurança para Internet**. 4ª ed. São Paulo: CERT.br, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 06 out. 2019.

CODE FOR BILLION. **Evolution of Internet of Things(IoT)**, 2017. Disponível em: <https://codeforbillion.blogspot.com/2017/10/evolution-of-internet-of-thingsiot.html>. Acesso em: 3 out. 2019.

COMPTIA. **Internet of Things Insights and Opportunities**, 2016. Disponível em: <https://www.comptia.org/resources/internet-of-things-insights-and-opportunities>. Acesso em: 24 set. 2019.

Cloud Security Alliance (CSA, 2016). **Future-Proofing the Connected World: 13 Steps to Developing Secure IoT Products**, 2016. Disponível em: <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf>. Acesso em: 26 out. 2019.

DANTAS, M. L. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. Olinda: Livro Rápido, 2011. Disponível em: http://www.marcusdantas.com.br/files/seguranca_informacao.pdf. Acesso em: 16 set. 2019.

EE TIMES. **Using MISRA C and C++ For Security and Reliability**, 2012. Disponível em: https://www.eetimes.com/document.asp?doc_id=1279810&page_number=2. Acesso em: 18 nov. 2019.

ELECTRONICS 360. **How Hackers Will Attack Your Embedded System and What You Can Do About It**, 2015. Disponível em: <https://electronics360.globalspec.com/article/5619/how-hackers-will-attack-your-embedded-system-and-what-you-can-do-about-it>. Acesso em: 18 nov. 2019.

EVANS, D. **A Internet das Coisas: Como a Próxima Evolução da Internet está Mudando Tudo**, CISCO, 2011. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf. Acesso em: 13 set. 2019.

FOWLER, M. **TestPyramid**, 2012. Disponível em: <https://martinfowler.com/bliki/TestPyramid.html>. Acesso em: 30 out. 2019.

GANESHAN, R. K. **Realizing a Forensic Cognizant Environment for Future IoT Research and Development by Designing a Secure Framework for the IoT Space**, 2017. Universidade de Bedfordshire, Bedford, 2017. Disponível em: https://www.researchgate.net/publication/316601151_Realizing_a_Forensic_cognizant_environment_for_future_IoT_Research_and_Development_by_designing_a_secure_framework_for_the_IoT_space. Acesso em: 19 set. 2019.

GARTNER. **Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor**, 2015. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2015-08-18-gartners-2015-hype-cycle-for-emerging-technologies-identifies-the-computing-innovations-that-organizations-should-monitor>. Acesso em: 19 set. 2019.

HANWHA TECHWIN. **Multi-directional Camera PNM-9084QZ**, 2019. Disponível em: <https://www.hanwha-security.com/en/products/camera/network/multi-sensor/PNM-9084QZ/overview/>. Acesso em: 12 nov. 2019.

HUREL, L. M.; LOBATO, L. C. **Segurança e privacidade para a Internet das Coisas**. Instituto Igarapé, Rio de Janeiro, p. 1–22, 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/11/Seguranca-e-Privacidade-para-a-Internet-das-Coisas.pdf>. Acesso em: 30 set. 2019.

INFORMATIONWEEK. **11 IoT Programming Languages Worth Knowing**, 2015. Disponível em: http://www.informationweek.com/mobile/mobile-applications/11-iot-programming-languages-worth-knowing/d/d-id/1319375?image_number=1. Acesso em: 18 nov. 2019.

LYRA, M. R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MANDEL, A.; SIMON, I.; DELYRA, J. L. Informação: Computação e Comunicação. **Revista USP**, São Paulo, n. 35, p. 12–45, 1997. Disponível em: <http://www.revistas.usp.br/revusp/article/view/26865>. Acesso em: 11 set. 2019.

MARTIN, J. A. **What is Shadow IoT? How to Mitigate the Risk**, 2019. Disponível em: <https://www.csoonline.com/article/3346082/what-is-shadow-iot-how-to-mitigate-the-risk.html>. Acesso em: 3 out. 2019.

MICROSOFT. **Melhores Práticas de Segurança para IoT**, 2018. Disponível em: <https://docs.microsoft.com/pt-br/azure/iot-fundamentals/iot-security-best-practices>. Acesso em: 18 nov. 2019.

MORAES, A. F. De. **Segurança em Redes: Fundamentos**. São Paulo: Érica, 2010.

NAZIR, M. **Study Warns of Security Gaps in Smart Light Bulbs**, 2019. Disponível em: <https://www.utsa.edu/today/2019/10/story/smartbulbs.html>. Acesso em: 17 nov. 2019.

NETWORK WORLD. **Largest DDoS Attack Ever Delivered by Botnet of Hijacked IoT Devices**, 2016. Disponível em: <https://www.networkworld.com/article/3123672/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html>. Acesso em: 12 nov. 2019.

O'REILLY, T. **What Is Web 2.0**, 2005. Disponível em: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>. Acesso em: 11 set. 2019.

Open Web Application Security Project (OWASP, 2018). **OWASP Internet of Things Project**, 2018. Disponível em: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. Acesso em: 2 out. 2019.

PAUL, F. **10 Principais Vulnerabilidades da Internet das Coisas**, 2019. Disponível em: <https://cio.com.br/10-principais-vulnerabilidades-da-internet-das-coisas/>. Acesso em: 2 out. 2019.

POPPER, K. R. **A Lógica da Pesquisa Científica**. São Paulo: Cultrix, 2013. Disponível em: <https://ocondedemontecristo.files.wordpress.com/2011/05/popper-karl-a-logica-da-pesquisa-cientifica.pdf>. Acesso em: 05 set. 2019.

Positivo Casa Inteligente. **Smart lâmpada Positivo**, 2019. Disponível em: <https://www.positivocasainteligente.com.br/conforto-e-automacao/smart-lampada/>. Acesso em: 17 nov. 2019.

RED HAT. **O Que é Segurança de APIs?**, 2019. Disponível em: <https://www.redhat.com/pt-br/topics/security/api-security>. Acesso em: 18 nov. 2019.

RIBEIRO, L. **Os Pilares da Segurança da Informação**, 2018. Disponível em: <https://nsworld.com.br/os-pilares-da-seguranca-da-informacao/>. Acesso em: 1 out. 2019.

SANTOS, B. P.; SILVA, L. A. M.; CELES, C. S. F. S.; BORGES, J. B. N.; PERES, B. S.; VIEIRA, M. A. M.; VIEIRA, L. F. M.; GOUSSEVSKAIA, O. N.; LOUREIRO, A. A. F. **Internet das Coisas: Da Teoria à Prática**, 2016. UFMG, Belo Horizonte. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>. Acesso em: 06 set. 2019.

SECURITY REPORT. **Câmeras Inteligentes: Falhas Permitem Acesso de Hackers**, 2018. Disponível em: <http://www.securityreport.com.br/overview/cameras-inteligentes-falhas-permitem-acesso-de-hackers/#.XcmQAjNKjIU>. Acesso em: 12 nov. 2019.

SÊMOLA, M. **Gestão da Segurança da Informação: Uma Visão Executiva**. Rio de Janeiro: Campus-Elsevier, 2013. Disponível em: <http://wiki.stoa.usp.br/images/7/79/Cap1-semola.pdf>. Acesso em: 16 set. 2019.

SHELBY, Z.; BORMANN, C. **6LoWPAN: The Wireless Embedded Internet**. Nova Jersey: Wiley, 2011.

SHOSTACK, A. **Threat Modeling : Designing for Security**. Indianapolis: Wiley, 2014. Disponível em: [https://moodle.ufsc.br/pluginfile.php/2377555/mod_resource/content/2/Threat Modeling.pdf](https://moodle.ufsc.br/pluginfile.php/2377555/mod_resource/content/2/Threat%20Modeling.pdf). Acesso em: 18 nov. 2019.

TANENBAUM, A. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Campus-Elsevier, 2003. Disponível em: [http://www.vazzi.com.br/arquivos_moodle/Redes de Computadores - Tanenbaum.pdf](http://www.vazzi.com.br/arquivos_moodle/Redes%20de%20Computadores%20-%20Tanenbaum.pdf). Acesso em: 11 set. 2019.

TECHTUDO. **Lâmpadas Smart podem estar vulneráveis a ataques de hackers**, 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/11/lampadas-smart-podem-estar-vulneraveis-a-ataques-de-hackers-diz-estudo.gh.html>. Acesso em: 11 nov. 2019.

TOBERGTE, D. R.; CURTIS, S. **Security Guidance for Critical Areas of Embedded Computing**, PRPL Foundation, 2013. Disponível em: <https://prplworks.files.wordpress.com/2016/01/prpl-security-guidance-for-critical-areas-of-embedded-computing-2-5-2.pdf>. Acesso em: 18 nov. 2019.

UVIASE, O.; KOTONYA, G. **IoT Architectural Framework: Connection and Integration Framework for IoT Systems**, 2018. Universidade de Lancaster, Lancaster. Disponível em: <https://arxiv.org/pdf/1803.04780.pdf>. Acesso em: 18 nov. 2019.

WORLD ECONOMIC FORUM. **The Global Risks Report 2018**, 2018. Disponível em: <http://reports.weforum.org/global-risks-2018/>. Acesso em: 30 set. 2019.