Comparativo de Protocolos de IoT para Automação Residencial: Potenciais Vulnerabilidades e Sugestões de Melhorias

Naiara Correa

Ciência da Computação – Universidade de Passo Fundo (UPF) – Campus I
Av. Brasil Leste, 285 - São José, Passo Fundo - RS, 99052-900

138729@upf.br

Abstract. *This article describes the research performed on the security of the Z-Wave and Thread protocols. Analyzing under aspects of the Information Security Principles and relating to their base standards, where incidents and discoveries of security breaches and vulnerabilities have been cited in some of them. In addition, successful attacks on both networks were reported to reinforce the idea of constant updates being extremely necessary. At the end of the article, suggestions for principles and/or security measures are presented with the intention of proposing ways to reduce and treat discovered breaches and vulnerabilities.*

Resumo. *Este artigo descreve a pesquisa realizada sobre a segurança dos protocolos Z-Wave e Thread. Analisando sob os aspectos dos Princípios da Segurança da Informação e fazendo uma relação com os seus padrões-base, onde foram citados incidentes e descobertas de falhas e vulnerabilidades de segurança em alguns deles. Adicionalmente foram relatados os ataques que foram bem-sucedidos em ambas as redes, de forma a reforçar a ideia de constantes atualizações serem extremamente necessárias. Ao final do artigo, são apresentadas sugestões de princípios e/ou medidas de segurança com a intenção de propor formas de reduzir e tratar as falhas e vulnerabilidades descobertas.*

1. Introdução

Cunhado no ano de 1999 por Kevin Ashton, mas já sendo desenvolvido e pesquisado muito antes, o termo Internet of Things (IoT) ou Internet das Coisas (IdC) surgiu da necessidade de se conectarem máquinas-à-máquinas (machine-to-machine) ou M2M e transmitirem informações através delas. O que na época era mais utilizado com propósitos de pesquisa ou essencialmente militares, hoje, em conjunto com a Inteligência Artificial, o Big Data, Analytics, a Robótica e tantos outros termos, já é visto como a Quarta Revolução Industrial, porque permitirá que concentremos a nossa atenção somente nas tomadas das decisões, enquanto que as máquinas ou *things* farão todo o trabalho braçal e repetitivo para nós, desde coletar, processar, transmitir e analisar dados e informações [1].

Segundo [2], até o segundo trimestre de 2018 já tínhamos cerca de 17,8 Bilhões de dispositivos conectados à internet, e destes, 7 Bilhões são dispositivos IoT, ou seja, que possuem a capacidade de se comunicar com outras máquinas (M2M). E as

previsões são de que até 2025 tenhamos 34,2 Bilhões de dispositivos conectados, sendo 21,5 Bilhões de dispositivos IoT.

No entanto, esse aumento expressivo de dispositivos conectados à internet é, ao mesmo tempo muito preocupante, pois muitos desses dispositivos são aparelhos comuns que temos dentro de casa ou que carregamos conosco, como smartphones, smart TVs, DVRs, câmeras de segurança, sensores de alarmes, fechaduras eletrônicas e outros, e isso sem contar os dispositivos IoT que estão sendo construídos e comercializados sem um controle rígido de avaliação dos produtos, ser ter ou sequer ter o mínimo de camadas de segurança necessários para proteger os donos de serem alvos de atacantes ou de terem seus dispositivos roubados remotamente, e dessa forma, serem usados por botnets para ataques de grandes proporções [3] [4].

Um dos maiores exemplos de ataques com botnets que ocorreu foi o caso Mirai , em que foi criado uma ferramenta capaz de infectar máquinas e direcioná-las para gerar tráfego em ataques com o objetivo de derrubar serviços e servidores. Inicialmente o objetivo era de obter lucro com o jogo Minecraft, mas um tempo depois, foi utilizado para derrubar serviços de streaming e de cloud, como Netflix, Spotify e Amazon [5]. Esse é apenas um dos ataques de grandes proporções, no entanto muitos outros causaram iguais e até inestimáveis prejuízos à empresas, indústrias, governos e, principalmente às pessoas. Este último, porque ainda são os alvos mais fáceis, por serem normalmente descuidadas, despreocupadas e/ou até não possuem a conscientização do impacto que as tecnologias têm em suas vidas.

Diante desse cenário, a tendência é a de crescimento nos investimentos na área de segurança em IoT. Segundo [6], a Gartner, empresa que divulga relatórios de pesquisas em diversos setores, estimou que até o final deste ano, os valores chegariam em torno de 1,5 bilhão de dólares, um aumento de cerca de 28% em relação ao ano passado. O que certamente abrem portas para novos investimentos na área.

Com vistas à proteger esses dispositivos e embarcar em um mercado em ascensão, inúmeras iniciativas surgiram propondo diferentes protocolos para serem utilizados nas implementações com dispositivos IoT [7]. O problema é que as diversidade não se encontram apenas na heterogeneidade dos tipos de dispositivos, mas também em fabricantes e nas implementações desses protocolos, o que acaba restringindo muito o universo IoT fazendo com que existam ilhas de comunicação entre estes dispositivos, pois somente protocolos que “falem a mesma língua”, ou seja, que tenham suporte ao mesmo protocolo, podem se comunicar. E essas comunicações não são somente muito importantes, mais sim, são essenciais para que se criem ambientes completamente inteligentes, autônomos e integrados, sejam dentro de casa, ou espalhados em uma *Smart City* (Cidade Inteligente) [8].

Por essas e outras razões que uma padronização e um consenso global é necessário para que sejam definidos quais os protocolos que serão amplamente utilizados e aceitos globalmente como forma de comunicação principal entre os diferentes dispositivos. Assim como foi feito com a internet, em que ao longo dos anos, foram sendo definidos quais protocolos seriam utilizados e/ou suportados e em quais camadas seriam implementados.

E esse trabalho, tem o objetivo de apresentar dois dos mais conhecidos e utilizados protocolos atualmente: Thread e Z-Wave. No entanto, o objetivo aqui, vai além de propor um consenso entre esses dois protocolos, mas sim, o de comparar e analisar sob a ótica dos Princípios da Segurança da Informação, se os protocolos

apresentados neste trabalho, possuem esses requisitos de segurança, adicionalmente será realizada uma relação dos protocolos com alguns padrões-base comuns aos dois, verificando das vulnerabilidades e falhas já descobertas neles e explicando do impacto disso para as redes desses protocolos. E ao final, serão apresentadas duas sugestões de princípios a serem seguidos e dois mecanismos para o controle e a manutenção da segurança nos protocolos de IoT.

Este trabalho começa fazendo uma breve introdução ao leitor da importância dos protocolos na Segurança da Internet das Coisas, explicando os dois escolhidos para comparação, na seção 2. Na seção 3 são realizadas análises dos protocolos de acordo com os Princípios da Segurança da Informação e traz uma análise das vulnerabilidade dos protocolos bases, na seção 4 são mencionadas as brechas de segurança já descobertas nos protocolo Z-Wave e Thread, a seção 5 são feitas sugestões de dois princípios e dois mecanismos que podem ser adotados de forma a mitigar novos ataques e novas brechas descobertas. Ao final, contém a conclusão da pesquisa realizada e as referências da mesma.

2. Protocolos Para Automação Residencial: Thread e Z-Wave

A Automação Residencial com IoT surgiu da ideia de utilizar a Internet em coisas (máquinas) para se comunicar automaticamente com pessoas e com outras máquinas a fim de realizar tarefas rotineiras e diárias, nos proporcionando maior conforto, segurança e produtividade [9].

De acordo com pesquisas, cerca de 80% dos dispositivos IoT no mundo inteiro estão vulneráveis à ataques de todos os tipos. E conforme já mencionado, o número desses dispositivos vêm crescendo exponencialmente, e com ela o número, a potência, a diversidade e o perigo que os ataques podem causar às pessoas, à privacidade e à segurança, como um todo [10].

Um ataque direcionado à uma residência, se realizado com sucesso, deixa o atacante de posse de todos os dados e informações que trafegam na rede doméstica, fotos, vídeos, mensagens, senhas, números e acessos à contas bancários, rotina e atividades diárias das pessoas, suas posses, seus bens, nomes e informações privadas dos membros da família, idades, endereços, telefones, e etc. Tendo posse desses dados e informações as possibilidades de ataques podem ser diversas, seja para roubar e vender no mercado negro informações privadas, seja para roubar e acessar contas bancárias, bens e propriedades, seja até para fazer chantagem em troca da divulgação ou da denúncia de possíveis atividades ilícitas realizadas pelas vítimas, ou pior ainda, ameaçar à familiares e amigos, caso as ordens dos atacantes não sejam cumpridas [11] [12] [13].

As possibilidades são inúmeras e são relativamente fáceis de se conseguir, visto que dispositivos conectados com a internet ou que possuem algum tipo de placa de rede, como eletrônicos e eletrodomésticos, normalmente são fabricados e desenvolvidos desconsiderando-se requisitos de segurança, e quando o fazem, dificilmente é pensando de forma a proporcionar segurança contra ataques de IoT.

Diante disso, vários protocolos surgiram com diferentes características, aplicações e propósitos [14]. A intenção aqui, não é a de apresentar e comparar todos,

por isso foram escolhidos dois protocolos para automação residencial - Z-Wave e Thread, respectivamente - que serão apresentados adiante.

2.1. Z-Wave

Z-Wave foi introduzido em 2001 e autorizado a ser utilizado pela Zensys, companhia Dinamarquesa. É um protocolo de comunicação de rede para dispositivos que operam com baixo custo e velocidade, e que pode ser adicionado à qualquer dispositivos eletrônico em uma casa. Em conjunto com seu grande adversário na área - ZigBee, que não será apresentado aqui - é um dos pioneiros na área de automação residencial para IoT, sendo muito utilizado e conhecido mundialmente com cerca de 94 milhões de dispositivos utilizando o protocolo. Especificamente elaborado para ser aplicado à automação residencial, tem um largura de banda limitada, com baixas taxas de transmissão, que opera em sua própria frequência, ou seja, suas transmissões não sofrem interferências de outros dispositivos.

Em 2005, foi construída uma aliança, chamada Z-Wave Alliance, que consistia em um consórcio entre empresas, com cerca de 500 membros, que produzem e distribuem produtos com o protocolo Z-Wave. A ideia do consórcio é expandir o número de aplicações para automação residencial que utilizem o protocolo Z-Wave, ampliando assim também a capacidade de interoperabilidade entre as aplicações, que funcionam somente entre produtos que também tenham suporte ao protocolo Z-Wave.

Uma rede Z-Wave suporte até no máximo 232 dispositivos, podendo ser utilizadas pontes ou *bridges* para ampliação deste número. Cada dispositivo da rede pode ser um de dois tipos apenas, um controlador, que vêm identificado assim através de um código vindo de fábrica, e um escravo, que não possuem identificação, pois é o controlador que lhe atribui uma ao inseri-lo em uma rede Z-Wave, que também possui identificação única, pois uma rede não pode se comunicar com outra e dispositivos de uma rede não podem enxergar os outros. Um rede pode ter mais de um controlador, no entanto, um principal deve ser definido.

A comunicação entre os dispositivos funciona através de acknowledges (ACK) que são enviados do controlador aos escravos, pelo menos três vezes, que dentro de um período de tempo devem responder aos chamados, caso contrários, sinais de falha são enviados ao usuário. O controlador possui uma tabela de rotas, onde ficam registrados todos os dispositivos da rede e quais outros dispositivos são acessados através deste, permitindo que, caso o controlador não tenha acesso (alcance) direto à algum dispositivo com o qual queria se comunicar, pode facilmente consultar esta tabela e calcular a rota (pulos de um nó a outro) até que algum deles tenha alcance e possa fazer o intermédio da comunicação.

Esse tipo de rede (topologia) é chamado de *redes mesh,* em que todos os nó (host/máquina/dispositivo) podem estar ao alcance de outros nós que estejam próximos, chamados de vizinhos, fazendo com que existam vários caminhos (rotas de um nó a outro) por onde é possível o alcance dos nós, gerando redundância dos links (caminhos) e garantia da consistência da rede. Além de permitir que o alcance máximo (tamanho do maior caminho) da rede seja ampliado, caso fosse utilizado uma topologia diferente, do tipo estrela ou árvore, por exemplo, em que o alcance é limitado aos nós mais próximos, apenas [15].

No caso da rede Z-Wave o alcance máximo que é possível chegar é de 100 metros, dentro da faixa de alcance permitido, que opera em diferentes frequências que mudam de região para região. No site da Silicon Labs, uma das empresas-membro da Z-Wave Alliance, mostra uma tabela com as diferentes faixas de operação para cada região do mundo, que variam de 865.2 na Índia à 926 no Japão, por exemplo. O que, conforme já foi mencionado, não causa interferências de/em outras redes, já que é uma faixa de rede própria do protocolo. E as suas transmissões operam na faixa de 9.6-100 kbps.

Redes Z-Wave podem conter todos os tipos de dispositivos, desde sensores de temperatura, de ambiente, de iluminação, lâmpadas, fechaduras, câmeras, switches, acessórios hospitalares, sistemas de segurança, sistemas HVAC, interfaces de computador, dispositivos de redes, termostatos, cortinas inteligentes, irrigadores de água, roteadores e muitos outros. Atualmente o site da Z-Wave Alliance informa que já são mais 2400 produtos interoperáveis através do protocolo Z-Wave, com cerca de 94 milhões de dispositivos no mundo [16] [17] [18].

2.2. Thread

Thread é um protocolo destinado para dispositivos 6LowPAN, explicado adiante, que operam em uma rede mesh IEEE 802.15.4. Surgiu como concorrente a outros protocolos que já existiam no mercado, como Z-Wave, com o propósito de oferecer algumas vantagens em relação a eles, por tratar alguns pontos de falhas descobertos em outros protocolos.

As vantagens relatadas pelos criadores, são: Simplicidade, instalação simples; Redes confiáveis, sem um ponto único de falha, por permitir que seus nós sejam dinamicamente arranjados na rede conforme as disponibilidades dos dispositivos; Segurança, todos as redes são autenticadas e as comunicações encriptadas; Eficiência, os dispositivos podem operar somente com a energia da bateria por anos, estando somente em modo *sleep* (repouso); Escalabilidade, as redes Thread podem ser facilmente escaláveis a centenas de dispositivos.

O protocolo Thread foi anunciado em 2014, pela Thread Group, aliança formada por empresas-líderes do setor do mercado de tecnologia, como Yale Security, Silicon Labs, Samsung Electronics, Nest Labs (uma subsidiária da Alphabet/Google), Freescale Semiconductor, Big Ass Fans and ARM, e recentemente a Apple anunciou o seu apoio também. Chegando em torno de 50 empresas participantes. O Thread Group é mantido através de uma taxa anual, exceto para licenças acadêmicas. Uma alternativa *open source* (de código aberto) para implementações de Thread é o OpenThread, lançado pela Nest Labs.

Recentemente uma nova aliança entre consórcios de protocolos foi anunciada, entre ZigBee Alliance e a Thread Group, a qual tem o propósito de unir as redes Thread e a linguagem implementada pela ZigBee como uma linguagem universalmente aceita por dispositivos IoT, chamada de *dotdot*.

O protocolo opera com base no padrão IEEE 802.15.4 e no padrão *6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks),* ou seja, com dispositivos com suporte ao protocolo de internet versão 6 (IPv6) que operem com baixos consumos de energia e que estejam interconectados dentro de uma pequena região conhecida como

PAN (Personal Area Network) ou Rede de Área Pessoal, que dentro das redes Thread, pode chegar à uma distância máxima de 100 metros.

Diferente das redes Z-Wave, as redes Thread operam com 2.4 GHz de frequência, o que pode causar interferências em redes Wi-Fi. Além de operarem com larguras de bandas de 250 kbps para transmissões de dados.

Assim como nas redes Z-Wave, as redes Thread também são mesh networks e também separam os nós em dois tipo, mas com características e funcionamentos diferentes: os *Routers* (roteadores), responsáveis pelas transmissões dos dados e pelos serviços de comissionamentos de novos dispositivos, e os *End Devices* (Dispositivos Finais), que se comunicam unicamente com o Router, pois não lhe são permitidos a retransmissão de dados para outros nós, como ocorre nas redes Z-Wave. Além disso, os dispositivos recebem outras formas de distinções de papéis para atuações dentro das redes.

A capacidade máxima permitida dentro da rede ultrapassa os 250 dispositivos. Qualquer dispositivo que seja 6LowPAN e que opere com o padrão IEEE 802.15.4, segundo a Thread Group, pode ser facilmente configurado e adicionado à rede Thread, sem necessidade de modificações no hardware, como ocorre com a Z-Wave [19] [20] [21] [22].

3. Análises Através de Comparativos entre os Protocolos

O presente tópico objetiva fazer uma análise comparativa de ambos os protocolos, tendo como base os Princípios da Segurança da Informação, definido por um padrão internacional, que será mencionado mais adiante. Além dessa análise foi feito um estudo das vulnerabilidades presentes em alguns dos padrões-bases comuns aos protocolos Z-Wave e Thread.

3.1. Análise Segundo os Princípios da Segurança da Informação

Nesta seção, conforme mencionado acima, serão abordados, os quesitos de segurança dos protocolos apresentados na seção 2, conforme os Princípios de Segurança da Informação, que objetivam definir métricas para que se possa avaliar o nível de segurança de um sistema como um todo, e assim definir melhores práticas tanto no processo de desenvolvimento de software, como também na definição das políticas de segurança da informação da empresa.

Segundo a Organização Internacional de Normalização (OIN) ou popularmente conhecida como ISO (*International Organization for Standardization*), que definiu os padrões a serem seguidos, através da ISO 17799:2005, são os seguintes: Disponibilidade, Integridade, Confidencialidade e Autenticidade, que serão abordados individualmente abaixo [23] [24] [25].

3.1.1. Disponibilidade

Sistemas precisam estar disponíveis o tempo todo, visto que momentos de quedas ou de falhas podem representar perdas de dados e informações ou ainda causar enormes prejuízos às empresas que tiverem planos e estratégias quanto à

disponibilidade dos seus sistemas. E no universo IoT isso não é diferente, muito pelo contrário, é uma necessidade maior ainda, pois para que as coisas (dispositivos) possam interagir uns com os outros e executarem tarefas automaticamente a qualquer tempo, é de extrema necessidade que os mesmos estejam disponíveis o tempo todo, seja processando tarefas no background ou aguardando comandos em modo *sleep*, que em outras palavras é quando um dispositivo se encontra em modo de economia de bateria ou energia [26] [27].

O protocolo Z-Wave, possui um modo de operação em que seus dispositivos chamados de controladores, assim definidos de fábrica através de um identificador único, que serve também para identificação individual da rede, permite à esse dispositivo o gerenciamento da rede, e a transmissão das mensagens. O que por si só, pode ser considerado como ponto único de falha, já que na ausência de um dispositivo controlador substituto, este pode ocasionar a falha e inoperação de todo a rede. Apesar disso, seus distribuidores, garantem que os dispositivos fabricados com o protocolo Z-Wave são otimizados para eficiência energética para que a bateria possa durar um ano ou mais [28].

Já o protocolo Thread, possui como dois pilares, a Eficiência e a Confiabilidade, em que prometem que os dispositivos de baixa energia de rede Thread, podem operar em modo *sleep* e operar somente com a energia da bateria por anos, além de garantir que a rede é protegida contra Pontos Únicos de Falha ou (*Single Point of Failure*), pois em sua própria configuração de nós da rede, seus dispositivos responsáveis por controlar, gerenciar e transmitir os dados são auto-elegíveis dinamicamente por tolerância à falhas, garantindo o funcionamento da rede, caso algum deles falhe ou não responda aos comandos [29].

3.1.2. Integridade

O segundo pilar da Segurança da Informação, o da Integridade, busca garantir que os dados ou informações armazenados ou transmitidos não estejam danificados, corrompidos ou alterados por indivíduos ou máquinas com o objetivo de causar perdas ou prejuízos. Assim como o pilar da disponibilidade, bem como os demais que serão apresentados, este também é de extrema importância, pois muitos dados trafegarão entre os dispositivos e em muitos casos serão utilizados para processamento, caso estes dados estejam alterados ou corrompidos isso pode causar o processamento por falhar e não permitir aos dispositivos completar as suas tarefas ou ainda por processar informações errôneas causando prejuízos e até danos físicos caso estes dispositivos venham a ser utilizados mal-intencionalmente [30].

No protocolo Z-Wave, a comunicação é realizada através de acknowledge ou ack, que são mensagem de retorno para informar ao remetente que a mensagem foi recebida. Após a confirmação, as mensagens são trocadas entre os nós. Isso garante que as mensagens enviadas serão recebidas, mesmo estando em modo *sleep*, as transmissões via rádio aguardam o dispositivo acordar e responder aos comandos. Quanto à integridade das mensagens contra alterações, as mensagens são encriptadas utilizando AES (Advanced Encryption Algorithm) ou Padrão de Criptografia Avançada com 128 bits de largura das chaves.

Em relação a este requisito no protocolo Thread, este utiliza uma camada de

enlace (*link layer*), que entre outras coisas, assegura a integridade da mensagem e replicação delas, através das especificações do padrão 802.15.4, com a adição de MLE (*Mesh Link Establishments*) handshakes (apertos de mão) entre os nós na camada MAC dos dispositivos para confirmar o recebimento das comunicações. No entanto o protocolo afirma que maiores camadas de segurança podem ser adicionadas na camada de aplicação. Outro problema relacionado ao protocolo Thread, é que ele confia nos protocolos Datagram Transport Layer Security (DTLS) e Transport Layer Security (TLS) com o objetivo de oferecer uma segurança fim-a-fim, no entanto esse tipo de segurança pesa no desempenho da rede, o que pode ocasionar lentidão, atrasos e até perdas de pacotes, isso sem levar em conta que alguns dispositivos podem não suportar tal especificação, no entanto a sua não implementação pode provocar impactos negativos em partes ou em toda a rede, causando uma grave falha de segurança [31].

3.1.3. Confidencialidade

Quanto à confidencialidade, este conceito é o responsável por certificar o real nível de segurança da rede, pois é através deste pilar que é garantido que as mensagens e os dados trafegados nela serão entregues com sigilo aos dispositivos autorizados [32].

No protocolo Z-Wave os três pilares são garantidos na camada de segurança, dentro das Classes de Comandos de Segurança, que basicamente são responsáveis por definir níveis de segurança à diferentes dispositivos e classificá-los, de acordo com as suas funcionalidades, em subclasses menores que utilizam a criptografia AES com 128 bits de largura.

Diferentemente do protocolo anterior, Thread, assegura a confidencialidade pela camada MAC, que se utiliza das chaves trocadas e configuradas nas camadas mais altas da aplicação. Esse protocolo também tira proveito da alta capacidade de criptografia *AES-CCM,* que é um contador com o método CBC-MAC (*cipher block chaining message authentication code*), utilizado para garantir a autenticidade nas criptografias que são transmitidas em suas mensagens.

3.1.4. Autenticidade

Por fim, o último dos pilares da Segurança da Informação, mas não o menos importante, é a autenticidade, o conceito que deve afirmar se determinado dispositivo ou indivíduo possui ou não acesso autorizado, seja para receber/transmitir dados ou mesmo para executar ou processar comandos [33].

Nas redes Z-Wave este pilar começa desde fábrica, com a transcrição de um Home-ID nos chips dos dispositivos considerados controladores. Além de identificá-los e distingui-los dos demais dispositivos, quanto para identificar a própria rede, visto que redes Z-Wave não podem se comunicar umas com as outras. O controlador, então define os Node-ID e atribui seu próprio Home-ID aos nós conforme for adicionando. Adicionalmente o método de Out-of-Band (OOB) Authentication é usado para operações de adição de novos dispositivos na rede. Isso garante que um outro canal seja utilizado para tal operação, evitando fraudes e ataques man-in-the-middle. No entanto, apesar da relativa segurança do protocolo como um todo, estudos e pesquisas, em implementações específicas da rede, identificaram que a mesma está exposta à ataques de interpersonificação de dispositivos já conhecidos, possibilitando o controle de alguns dispositivos menos seguros da rede.

O protocolo Thread, que também se utiliza do método de autenticação OOB, garante que nenhum dispositivo entra na rede sem ser autenticado e ter suas mensagens encriptadas e seguras. Um dos mecanismos de segurança do protocolo Thread é a ofuscação dos endereços IP e MAC dos dispositivos, randomizando-os. Após a fase de inclusão, os nós são identificados, ou através desses mesmos endereços randomizados ou através de uma parte do ID do nó. Além disso uma chave é utilizada para autenticação e encriptação na camada MAC. No entanto se utiliza de padrões com vulnerabilidades conhecidas, como na camada MAC do protocolo 802.15.4 [34], utilizada para garantir a segurança dos frames, que é usada no protocolo para identificar e autenticar um dispositivo da rede Thread [35].

3.2. Análise dos Protocolos Bases

Para que os protocolos Z-Wave e Thread possam ser capazes de cumprir com as demandas do mercado e de realmente conectarem tantos equipamentos conforme ofertam e prometem, é necessário que possuam outros padrões definidos internamente para que possam se comunicar e operar adequadamente e com segurança, tanto entre camadas quanto entre dispositivos.

E para isso uma gama de protocolos-bases de ser definida, independente de ser um protocolo construído do zero ou que utilize como base outros padrões conhecidos, para que seja compatível com os padrões da internet e dos dispositivos já comercializados, é necessário que tenham alguma base em padrões já existentes e utilizados. O que pode abrir novas brechas de segurança, pois isso implica que tais protocolos-base por já serem conhecidos e implementados, já tem as suas vulnerabilidades também conhecidas, exploradas e estudadas.

Farei, portanto, neste tópico uma breve citação das vulnerabilidades já conhecidas de alguns dos padrões suportados pelos protocolos aqui apresentados, e ao final desta secção uma análise das implicações e potenciais impactos de tais falhas e vulnerabilidades para cada uma das redes.

3.3.1. G.9959

É uma recomendação do setor de radiocomunicação (ITU-R) para as camadas física e de controle de acesso ao meio, PHY e MAC, respectivamente, para dispositivos de curto alcance com bandas-estreitas de radiocomunicações. É o protocolo-base dos produtos implementados com Z-Wave [36].

Um estudo que avaliou a Rec. G.9959 em redes com infraestruturas críticas, determinou que pelo menos três classes de ataques são possíveis: 1) Ataques de reconhecimento, em que um usuário mal-intecionado com uma antena high-gain (HGA) poderia facilmente coletar dados e informações da rede sem ser notado; 2) Ataques de Denial-of-Service (DoS) fazendo *jamming* nas transmissões de banda-estreita da rede; 3) Ataques de Injeção de Pacotes, através do primeiro ataques (de reconhecimento) pode facilmente enviar comandos legítimos na rede e anular as mensagens originais.

Esse estudo foi realizado em redes Z-Wave, e maiores detalhes técnicos das implementações dos ataques e das ferramentas utilizadas, bem como dos dados e das informações coletadas podem ser obtidas no estudo [37].

3.3.2. IEEE 802.15.4

É um protocolo definido em 2003 pelo IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) para dispositivos de baixa taxas de transferências que operem em redes pessoais sem fio. Esse protocolo especifica a camada física (PHY) e o controle de acesso ao meio (MAC). É citado como padrão-base para o protocolo Thread [38].

Em um estudo sobre as vulnerabilidades encontradas na especificação deste protocolo [39], foram descobertas brechas de segurança em relação ao gerenciamento IV, onde seria possível, com uma mesma chave a utilização de muitas entradas ACL (*Access Control List*), além da não garantia das tabelas de nonces durante quedas de energia ou em modo de operação com baixa energia (*sleep mode*). A segunda falha na especificação do protocolo foi em relação ao suporte inadequado da tabela ACL para os diferentes modelos de chaves. E a terceira se refere à insuficiência na proteção da integridade, quanto, por exemplo aos retornos dos pacotes de *acknowledgment*.

3.3.3. 6LoWPAN

É um protocolo do Internet Engineering Task Force (IETF) que tem por objetivo definir os padrões de implementações para que dispositivos com capacidade de recursos limitados, definidos pelo padrão 802.15.4, possam atuar sobre o Protocolo de Internet Versão 6 (IPv6) e assim participar da Internet das Coisas (IdC). O protocolo define os procedimentos a serem seguidos para o encapsulamento e compressão de cabeçalhos nos pacotes IPv6 [40].

Uma análise de segurança do mecanismo de fragmentação do protocolo 6LoWPAN identificou dois ataques possíveis em redes com suporte à esse protocolo, em que foram explorados os recursos escassos de memória e a falta de autenticação na camada 6LoWPAN, que fica entre as camadas de rede e de enlace.

Um das vulnerabilidades deste protocolo é que, ele por si só, ou seja, em sua própria camada, não consegue identificar se os fragmentos que chegam, pertencem ao mesmo remetente ou não. O que possibilita que o atacante possa duplicar, alterar ou soltar pacotes legítimos. Outra vulnerabilidade, se refere ao buffer reservado para a montagem dos fragmentos após todos chegarem. A falha aqui é que devido ao seu tamanho reduzido, somente os pacotes considerados completos são aceitos, pacotes com defeitos ou incompletos são recusados, o que abre brechas para ataques de DoS [41].

3.3.3. Advanced Encryption Standard (AES)

Originalmente de nome Rijndael, é um padrão de criptografia avançado aprovado Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA em 2001 e adotado pelo governo americano, sendo utilizado mundialmente para transações bancárias e operações online com segurança. O padrão decripta os dados em blocos de 128 bits, mas tem suporte a chaves simétricas de tamanhos 128, 192 e 256 bits de comprimento. É o protocolo padrão implementado por ambos os protocolos Z-Wave e Thread, no entanto o tamanho *AES*-128 é o utilizado no protocolo Z-Wave. Enquanto que o Thread utiliza o AES-CCM (contador com CBC-MAC), que é um modo de operação que trabalha com blocos de 128 bits de forma a poder garantir a autenticação e a confidencialidade [42].

É uma das criptografias mais utilizadas no mundo por ser uma das mais seguras. Um ataque de força bruta dificilmente quebraria uma chave de 128 bits de largura,

mesmo considerando uma enorme capacidade computacional, ainda assim segundo estudos levaria 1 bilhão bilhão de anos, o que já é muito maior do que a idade da terra com 13.75 bilhões anos [43].

Uma pesquisa recente, desenvolvida por criptoanalistas da Microsoft em parceria com uma universidade da Bélgica, em cima da criptografia *AES*-256 descobriu que é possível acelerar o tempo de processamento de três a cinco vezes mais rápido, mas ainda assim três ou quatro vezes a idade da terra ainda é um tempo impraticável. Portanto, é seguro afirmar que a criptografia utilizada por ambos os protocolos é uma das seguras do mundo. No entanto, a criptografia por si só não dá garantias de que a rede é segura, apenas que os dados ou informações que estiverem cifrados, estão, mas apenas se o atacante não tiver acesso às chaves privadas também [44].

3.3.4. Internet Protocol Version 6 (IPv6)

É nova versão do Protocolo de Internet (versão 6 - IPv6), com o objetivo de substituir a atual (versão 4 - IPv4), cujos 4 bilhões de endereços de IP já terminaram. A nova versão suporta cerca de 340 undecilhões ou sextilhões de endereços, e tem endereçamento de 128 bits (o quádruplo do IPv4). O IPv6 é nativo tanto na Z-Wave quanto na Thread, e ambos oferecem suporte ao IPv4 [45].

No entanto, muitas vulnerabilidades já foram encontradas nessa nova versão, dentre elas a possibilidade de ser realizado ataques de DoS através dos mecanismos de fragmentação ou de descoberta de vizinhos realizada com multicast. Outra vulnerabilidade inclui a possibilidade da manipulação dos cabeçalhos estendidos, que poderia levar à ataques DoS ou serem utilizados para evitar firewalls ou Sistemas de Prevenção de Intrusões (IPS). Portanto não necessariamente o novo protocolo de internet é mais seguro, mas simplesmente possui maior capacidade de endereçamento que o seu antecessor [46].

3.3.5. DTLS (Data Transport Layer Security)

É um protocolo de comunicação designado para garantir a segurança dos protocolos de datagramas, baseado no Transport Layer Security (TLS). Tem o objetivo de prevenir *eavesdropping,* adulteração e falsificação de mensagens. Apesar disso, utiliza UDP ao invés de TLS, o que lhe dá ganho em performance, mas ao mesmo tempo tem de lidar com perdas e reordenação de pacotes. Thread utiliza este protocolo para prover autenticação e credenciais de acesso. No protocolo Z-Wave é utilizado para assegurar as comunicações entre os hosts *LAN* e os nós Z-Wave [47].

Uma vulnerabilidade no protocolo TLS foi encontrada, na qual o DTLS é baseado, e consistia em manipular campos de preenchimento para causar atrasos nas respostas e com isso recuperar textos puros em implementações deste protocolo com o OpenSSL. Apesar do protocolo DTLS ser baseado no TLS, mas utiliza UDP, muitos dos requisitos de segurança do TLS não são implementados, no entanto, um estudo demonstrou que mesmo sem as mensagens de erros do TLS, cruciais para o sucesso do ataque, ainda assim é possível que o ataque seja cumprido, se os tempos das injeções dos pacotes forem cuidadosamente manipulados [48].

Diante das vulnerabilidades apresentadas, é possível observar que os impactos para as redes que implementam esses padrões-bases podem ser muito prejudiciais e bastante diversos, se levado em conta que muitas vulnerabilidades envolvem ataques de

negação de serviços, e que tantas outras possuem detalhes técnicos minuciosos, mas que se conhecidos e atacados, podem desestabilizar partes ou toda a rede. Outros ataques, além de possibilitarem o domínio da rede, podem levar à causar desastres e acidentes fatais, se os dispositivos sob controle forem manuseados com más-intenções ou sem o conhecimento das suas implicações nos ambientes externos, como uma manipulação remota de objetos com defeitos pode ocasionar acidentes com os usuários das redes. Ou ainda obter lucros com a venda e/ou extorsão dos dados e informações roubados.

4. Ataques bem-sucedidos

Falhas e vulnerabilidades são inevitáveis considerando-se o enorme conjunto de protocolos, ferramentas e tecnologias que compõe cada uma das redes. Tais falhas não somente podem estar na especificação dos protocolos, mas também podem vir de implementações incompletas ou equivocadas, ou ainda, de erros ainda não descobertos ou sem muitas alternativas viáveis de se corrigir. Tudo isso impacta nas redes e nos dispositivos envolvidos nela.

4.1. Z-Wave

Um exemplo de ataque remoto com potencial dano aos dispositivos físicos foi relatado em uma conferência em que os criadores de uma ferramenta, para realizar Pen-Testing em redes Z-Wave, mostraram como é relativamente simples, diante do acesso à esses dispositivos, enviar comandos rápidos de modo a alterar o funcionamento dos mesmos para que venham a ser danificados ou até mesmo destruídos, como foi o exemplo em que eles apresentaram ser possível destruir lâmpadas fluorescentes com comandos rápidos de ligar e desligar. E que apesar do protocolo ter suporte à uma criptografia relativamente segura, conforme já mencionado, a implementação dela, depende dos fabricantes de dispositivos. Na pesquisa, foram testados 33 produtos Z-Wave, mas somente 9 deles implementaram criptografia [49].

Um outro caso, em maio deste ano, ocorreu um vazamento de uma vulnerabilidade encontrada na rede Z-Wave em que era possível reduzir o nível de segurança de um dispositivo e com isso facilitar a dominação dos dispositivos aos seus atacantes. No entanto, a Z-Wave Alliance apenas afirmou que tomaria medidas de forma a informar ou notificar melhor seus usuários sobre o que suas ações poderiam vir a causar. Sem sequer tratar a falha como crítica ou mesmo uma vulnerabilidade do protocolo [50].

4.2. Thread

Diferentemente da rede Z-Wave, que está no mercado desde 2001 e possui milhões de dispositivos no mundo todo, a rede Thread, lançada em 2004, ainda possui poucos estudos, em especial sobre a sua segurança e potenciais falhas, no entanto foi possível encontrar uma análise feita sobre a rede Thread através de ataques eletromagnéticos (EM), feitos com certa proximidade, em que são feitas análises sob a radiação eletromagnética emitidas pelos dispositivos com o objetivo de capturar chaves criptográficas. Nesse estudo o atacante pode obter total controle da rede, simplesmente escutando e analisando as trocas de informações sobre as chaves MLE entre os dispositivos pai e filho. De posse das chaves, o dispositivo pode escutar e participar da rede, bem como elevar seu nível até o ponto em que não somente pode adicionar mais nós à rede, mas também pode alterar os parâmetros da mesma de forma que o proprietário da rede perca total controle sobre a mesma [51].

O objetivo dessa seção foi o de explanar os ataques que foram bem-sucedidos em ambas as redes, de forma a reforçar a ideia de que as atualizações de seguranças são tão importantes quanto a própria implementação das redes, e que devem ser realizadas de forma contínua e realizadas com certa frequência.

5. Sugestões de Princípios da Segurança da Internet das Coisas

Conforme o mercado de IoT vai se expandindo, novas discussões sobre as questões de segurança vão surgindo, e com elas novos parâmetros, sugestões, e desafios vão sendo propostos. E até que haja uma entidade internacional para normalizar esses padrões e suas práticas de segurança em dispositivos IoT, da mesma forma que a ISO normaliza os Princípios de S.I. em sistemas de modo geral, os princípios necessários à segurança em IoT acabam ficando em aberto até que uma padronização seja adotada.

Por isso, pela diversidade de sugestões encontradas e pelas minhas próprias observações à respeito das implementações dos protocolos, trago aqui, uma seleção de alguns princípios que identifiquei como mais importantes considerando apenas à nível de implementações de protocolos para dispositivos IoT, que é o abordado neste trabalho. No entanto, níveis e princípios de segurança devem ser abordados e adotados em todas as camadas de um dispositivo IoT, desde o processo de fabricação do hardware até o processo de desenvolvimento de software.

3.2.1. Privacidade dos Dados

A privacidade dos dados, se refere aos dados pessoais que são coletados e da forma como são utilizados. No últimos anos, várias organizações tiveram suas aplicações invadidas e os dados de milhões de pessoas vazados e expostos na rede ou vendidos à organizações criminosas ou com propósitos de marketing direcionado [52]. Isso cria outra preocupação em relação as redes de aparatos inteligentes, que é o tratamento, armazenamento, uso e descarte dos dados e informações pessoais dos usuários da rede. Ou seja, não basta a rede possuir mecanismos para garantir a confidencialidade, mas também deve ser capaz de ser transparente quanto à isso, e caso a rede seja invadida, deve existir uma forma de operação que, em último caso, tente assegurar a proteção desses dados.

5.2. Heterogeneidade dos Dispositivos e Recursos Limitados

De um modo geral, como já foi dito, seriam necessários diversos níveis de segurança, para que a rede, como um todo, pudesse ser considerada segura o suficiente para resistir aos diversos ataques que uma rede doméstica de dispositivos IoT pode sofrer, no entanto, é impraticável garantir a segurança contra todos os tipos e níveis de ataques, até porque, muitas vulnerabilidades ainda são desconhecidas ou ainda não foram exploradas, no entanto, um outro fator entra em consideração quando se trata de dispositivos IoT.

Esses *devices,* como são chamados em inglês, como já explicado na introdução, podem ter diferentes propósitos e funções, até porque é a diversidade deles e as suas capacidades que compõem a chamada Internet das Coisas, no entanto isso também implica que a própria natureza desses dispositivos é uma restrição à implementação de níveis e camadas de segurança apropriados, pois muitos deles sequer tem recursos como memória, largura de banda ou energia suficientes para isso [53]. O que não somente

impacta e limita a implantação de redes de IoT seguras como também requer que os protocolos sejam capazes de lidar e operar com as diferentes limitações impostas, sendo também, habilitados à identificar, distinguir e limitar as atuações e acessos para cada tipo de dispositivo, de acordo com o nível de segurança que possui.

5.3. Políticas de Atualização dos Mecanismos de Segurança

Conforme novas ameaças forem surgindo e o número de equipamentos IoT aumentando significativamente, seria bastante interessante que os criadores/mantenedores dos protocolos fizessem constantes patches de atualizações de seguranças em seus dispositivos, para que possam garantir a proteção dos usuários, de seus equipamentos e dos dados e informações pessoais trafegados na rede.

5.4. Auditoria e Licenciamento de dispositivos IoT

Outra forma de garantir que ao menos os Princípios de S.I. sejam cumpridos, seria o de propor formas de auditoria de segurança e qualidade em dispositivos IoT, avaliando se os requisitos básicos de implementações dos protocolos foram cumpridos, e caso sejam, realizar o licenciamento de tais dispositivos, forçando os fabricantes a realizar as implementações necessárias.

6. Conclusão

Neste trabalho foram apresentados os protocolos Z-Wave e Thread, e realizadas a análises dos mesmos em relação aos Princípios de Segurança da Informação. Adicionalmente foram apresentadas as vulnerabilidades já descobertas dos padrões-bases de ambos os protocolos, e à partir desse ponto perceber que a gama de ataques é muito maior do que as especificações de um único protocolo, e não se restringe somente a ele, mas acaba incorporando as falhas e vulnerabilidades das suas implementações utilizadas como base também. E não necessariamente por não serem seguros o suficiente, mas porque precisam que seus requisitos sejam constantemente revisados e atualizados, o que pode ser comprovado na seção em que ataques bem-sucedidos foram relatados. Além das vulnerabilidades dos padrões-bases, foram citados, pelo menos, dois casos de vulnerabilidades descobertas na rede Z-Wave com grandes potenciais. E ao final foram introduzidos algumas sugestões de Princípios de Segurança para os Dispositivos da Internet das Coisas, que podem ser incorporados aos protocolos aqui discutidos.

Referências

1. INTERNET DAS COISAS. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Internet_das_coisas&oldid=53604902>. Acesso em: 15 nov. 2018.

2. LUETH, K. L. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. IoT Analytics, 2018. Disponivel em: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>. Acesso em: 07 nov. 2018.

3. COSSETTI, M. C. Brasil é líder em ataques a dispositivos IoT com 30 mil infectados em 2018. Tecnoblog, 2017. Disponivel em:

<https://tecnoblog.net/256165/brasil-e-lider-em-ataques-a-dispositivos-iot-com-30-mil-infectados-em-2018/>. Acesso em: 07 nov. 2018.

4. HIGA, P. Um dos maiores ataques DDoS da história foi feito com câmeras de segurança. Tecnoblog, 2018. Disponivel em: <https://tecnoblog.net/201789/ddos-camera-seguranca-iot/>. Acesso em: 07 nov. 2018.

5. VENTURA, F. A botnet que gerou caos no ano passado foi feita para derrubar servidores de Minecraft. Tecnoblog, 2017. Disponivel em: <https://tecnoblog.net/229999/criadores-botnet-mirai-minecraft/>. Acesso em: 07 nov. 2018.

6. CONVERGÊNCIA DIGITAL. Ataques elevam investimentos em segurança de IoT para US$ 1,5 bilhão. Convergência Digital, 2018. Disponivel em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite&infoid=47604&sid=18>. Acesso em: 07 nov. 2018.

7. MORALES, Joshua O. et al. A Comparative Study of Thread Against ZigBee,Z-Wave, Bluetooth,and Wi-Fi as a Home-Automation Networking Protocol. . [20--]. 7 p. Dissertation (Data Networks and Communication)- Asia Pacific College, Makati, Philippines, 2016. Disponível em: <https://www.researchgate.net/publication/309669667_A_Comparative_Study_of_Thread_Against_ZigBee_Z-Wave_Bluetooth_and_Wi-Fi_as_a_Home-Automation_Networking_Protocol>. Acesso em: 07 nov. 2018.

8. MARKSTEINER, Stefan et al. An overview of wireless IoT protocol security in the smart home domain. **2017 Internet Of Things Business Models, Users, And Networks**, [s.l.], p.2-10, nov. 2017. Disponível em: <https://arxiv.org/pdf/1801.07090.pdf>. Acesso em: 07 nov. 2018.

9. SCHNEIDER, S. Understanding The Protocols Behind The Internet Of Things. Electronic Design, 2013. Disponivel em: <https://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things>. Acesso em: 11 nov. 2018.

10. RAMBUS. Smart Home: Threats and Countermeasures. Rambus. Disponivel em: <https://www.rambus.com/iot/smart-home/>. Acesso em: 11 nov. 2018.

11. GODHA, Rahul; PRATEEK, Sneh; KATARIA, Nikhita. Home Automation: Access Control for IoT Devices. **International Journal Of Scientific And Research Publications.** [s. L.], p. 555-558. out. 2014. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.1513&rep=rep1&type=pdf#page=556>. Acesso em: 11 nov. 2018.

12. WRITER, G. The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. IoT For All, 2017. Disponivel em: <https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>. Acesso em: 11 nov. 2018.

13. TELECOM ASIA. Home Wi-Fi routers, IoT devices targeted in attacks. Telecom Asia, 2018. Disponivel em: <https://www.telecomasia.net/content/home-wi-fi-

routers-iot-devices-targeted-attacks>. Acesso em: 11 nov. 2018.

14. PARRISH, K. ZigBee, Z-Wave, Thread and WeMo: What's the Difference? Tom's Guide, 2017. Disponivel em: <https://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html>. Acesso em: 11 nov. 2018.

15. REDES MESH. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Redes_Mesh&oldid=52737683>. Acesso em: 24 jul. 2018.

16. Z-WAVE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2016. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Z-Wave&oldid=46510349>. Acesso em: 22 ago. 2016.

17. VESTERNET. Understanding Z-Wave Networks, Nodes & Devices. Vesternet. Disponivel em: <https://www.vesternet.com/resources/technology-indepth/understanding-z-wave-networks/>. Acesso em: 11 nov. 2018.

18. Z-WAVE ALLIANCE. Z-Wave Products. Disponivel em: <https://products.z-wavealliance.org/>. Acesso em: 11 nov. 2018.

19. Thread (network protocol). In: Wikipedia, The Free Encyclopedia. Flórida: Wikimedia Foundation, 2016. Disponível em: <https://en.wikipedia.org/w/index.php?title=Thread_(network_protocol)&oldid=866789491>. Acesso em: 22 ago. 2016.

20. OPEN THREAD. Node Roles and Types. Open Thread. Disponivel em: <https://openthread.io/guides/thread-primer/node-roles-and-types>. Acesso em: 11 nov. 2018.

21. SAN RAMON, C. Introducing Thread: A New Wireless Networking Protocol For The Home. Thread Group, 2014. Disponivel em: <https://www.threadgroup.org/news-events/press-releases/ID/20/Introducing-Thread-A-New-Wireless-Networking-Protocol-for-the-Home>. Acesso em: 11 nov. 2018.

22. SPEAK DOTDOT. Dotdot Story. Speak dotdot. Disponivel em: <https://www.speakdotdot.com/dotdot-over-thread/>. Acesso em: 11 nov. 2018.

23. SEGURANÇA DA INFORMAÇÃO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Seguran%C3%A7a_da_informa%C3%A7%C3%A3o&oldid=53598455>. Acesso em: 15 nov. 2018.

24. MOREIRA, E. Conheça os pilares da Segurança da Informação. Introduceti, 2017. Disponivel em: <http://introduceti.com.br/blog/pilares-da-seguranca-da-informacao/>. Acesso em: 11 nov. 2018.

25. ISO/IEC 17799. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2017. Disponível em: <https://pt.wikipedia.org/w/index.php?title=ISO/IEC_17799&oldid=49227468>. Acesso em: 6 jul. 2017.

26. SISTEMA DE ALTA DISPONIBILIDADE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2015. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Sistema_de_alta_disponibilidade&oldid=44151807>. Acesso em: 9 dez. 2015.

27. FCAMARA. Entenda o papel da alta disponibilidade e performance dos sistemas. Fcamara, 2017. Disponivel em: <http://blog.fcamara.com.br/entenda-o-papel-da-alta-disponibilidade-e-performance-dos-sistemas/>. Acesso em: 11 nov. 2018.

28. SMARTER HOME. Advantages of Z-Wave. Smarter Home. Disponivel em: <https://smarterhome.sk/en/informacie/advantages-of-z-wave-10>. Acesso em: 11 nov. 2018.

29. OPEN THREAD. What is Thread? Open Thread. Disponivel em: <https://openthread.io/guides/thread-primer>. Acesso em: 11 nov. 2018.

30. INTEGRIDADE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Integridade&oldid=53051226>. Acesso em: 3 set. 2018.

31. SILICON LABS (Org.). **UG103.11:** Thread Fundamentals. Disponível em: <https://www.silabs.com/documents/public/user-guides/ug103-11-appdevfundamentals-thread.pdf>. Acesso em: 11 nov. 2018.

32. CONFIDENCIALIDADE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2017. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Confidencialidade&oldid=48523421>. Acesso em: 11 abr. 2017.

33. AUTENTICIDADE. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Autenticidade&oldid=51849983>. Acesso em: 19 abr. 2018.

34. MOINUDDIN, Khaja et al. A Survey on Secure Communication Protocols for IoT Systems. **International Journal Of Engineering And Computer Science.** Ballari, India, p. 1-6. jul. 2017. Disponível em: <https://www.ijecs.in/index.php/ijecs/article/download/2977/2756/>. Acesso em: 24 nov. 2018.

35. THREAD GROUP. Thread Stack Fundamentals. Thread Group, 2015. Disponivel em: <https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=633>. Acesso em: 11 nov. 2018.

36. INTERNATIONAL TELECOMMUNICATION UNION. **RECOMMENDATION ITU-T G.9959**: Short range narrow-band digital radiocommunication transceivers – PHY and MAC layer specifications. 2012. 126 p. Disponível em: <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9959-201202-S!!PDF-E&type=items>. Acesso em: 24 nov. 2018.

37. Z-WAVE ALLIANCE. Z-Wave Transceivers – Specification of Spectrum Related Components. Z-Wave Alliance. Disponivel em: <https://z-wavealliance.org/wp-content/uploads/2015/02/ZAD12837-1.pdf>. Acesso em: 11 nov. 2018.

38. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 802.15.4**: IEEE 802.15 WPAN™ Task Group 4 (TG4). 2018. Disponível em: <http://www.ieee802.org/15/pub/TG4.html>. Acesso em: 24 nov. 2018.

39. ACM WORKSHOP ON WIRELESS SECURITY (WISE 2004), 2004, Philadelphia, Pa, U.s.a.. **Security Considerations for IEEE 802.15.4 Networks.** Berkeley: University Of California, 2004. 11 p. Disponível em: <https://people.eecs.berkeley.edu/~daw/papers/15.4-wise04.pdf>. Acesso em: 24 nov. 2018.

40. OLSSON, Jonas. **6LoWPAN demystified.** Texas: Texas Instruments, 2014. 13 p. Disponível em: <http://www.ti.com/lit/wp/swry013/swry013.pdf>. Acesso em: 24 nov. 2018.

41. 6TH ACM CONFERENCE ON SECURITY AND PRIVACY IN WIRELESS AND MOBILE NETWORKS (WISEC '13), 13., 2013, Budapest, Hungary. **6LoWPAN Fragmentation Attacks and Mitigation Mechanisms.** Germany: Rwth Aachen University, 2013. 12 p. Disponível em: <https://www.researchgate.net/publication/259184554_6LoWPAN_Fragmentation_Attacks_and_Mitigation_Mechanisms>. Acesso em: 24 nov. 2018.

42. ROUSE, Margaret. **Advanced Encryption Standard (AES).** 2017. Disponível em: <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>. Acesso em: 24 nov. 2018.

43. ARORA, Mohit. **How secure is AES against brute force attacks?** 2012. Disponível em: <https://www.eetimes.com/document.asp?doc_id=1279619>. Acesso em: 18 nov. 2018..

44. THE CONVERSATION (Org.). **World's toughest encryption scheme is 'vulnerable' … so what about you?** 2011. Disponível em: <https://theconversation.com/worlds-toughest-encryption-scheme-is-vulnerable-so-what-about-you-2958>. Acesso em: 18 nov. 2018.

45. MOREIRAS, Antonio M.. **IPv6 A nova geração do Protocolo Internet.** Rio Preto: Semana de Tecnologia e Iii Jornada de Pesquisa, 2008. 60 slides, color. Disponível em: <http://www.ceptro.br/pub/CEPTRO/PalestrasPublicacoes/IPv6-semanatec.pdf>. Acesso em: 18 nov. 2018.

46. DAWOOD, Harith A.. IPv6 Security Vulnerabilities. **International Journal Of Information Security Science.** Erbil, Iraq, p. 100-105. dez. 2012. Disponível em: <http://www.ijiss.org/ijiss/index.php/ijiss/article/view/16/100-105>. Acesso em: 18 nov. 2018.

47. INTERNET ENGINEERING TASK FORCE (IETF). **REQUEST FOR COMMENTS: 6347**: Datagram Transport Layer Security Version 1.2. [s.i.], 2012. Disponível em: <https://tools.ietf.org/html/rfc6347>. Acesso em: 18 nov. 2018.

48. 19TH ANNUAL NETWORK & DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, 2012, San Diego. **Plaintext-Recovery Attacks Against Datagram TLS.** Egham, Surrey: University Of London, 2012. 18 p. Disponível em: <http://www.isg.rhul.ac.uk/~kp/dtls.pdf>. Acesso em: 18 nov. 2018.

49. SMITH, Ms.. **EZ-Wave: A Z-Wave hacking tool capable of breaking bulbs, abusing Z-Wave devices.** 2016. Disponível em: <https://www.csoonline.com/article/3024217/security/ez-wave-z-wave-hacking-tool-capable-of-breaking-bulbs-and-abusing-z-wave-devices.html>. Acesso em: 24 nov. 2018.

50. SPRING, Tom. **Millions of IoT Devices Vulnerable to Z-Wave Downgrade Attacks, Researchers Claim.** 2018. Disponível em: <https://threatpost.com/millions-of-iot-devices-vulnerable-to-z-wave-downgrade-attacks-researchers-claim/132295/>. Acesso em: 24 nov. 2018.

51. DINU, Daniel; KIZHVATOV, Ilya. EM Analysis in the IoT Context: LessonsLearned from an Attack on Thread. **Acr Transactions On Cryptographic Hardware And Embedded Systems.** [s.l.], p. 73-97. fev. 2018. Disponível em: <https://tches.iacr.org/index.php/TCHES/article/view/833/785>. Acesso em: 24 nov. 2018.

52. ARMERDING, Taylor. **The 17 biggest data breaches of the 21st century.** 2018. Disponível em: <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>. Acesso em: 24 nov. 2018.

53. 2015 10TH INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS (ICITST), 2015, Sharjah. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. [s.l.]: American University Of Sharjah, 2015. 9 p. Disponível em: <https://www.researchgate.net/publication/300413927_Internet_of_things_IoT_security_Current_status_challenges_and_prospective_measures>. Acesso em: 24 nov. 2018.