IOT – INTERNET DAS COISAS

AULA 6

Prof. Gian Carlo Brustolin

CONVERSA INICIAL

Até aqui, alertamos sobre os problemas de segurança ligados ao uso desta tecnologia de internet das coisas. Como muitas incertezas pairam sobre IoT, natural é que ainda não se conheçam, plenamente, as vulnerabilidades que ela apresenta ou mesmo que apresentará, já que IoT ainda é uma criança tecnológica. De qualquer forma, chegou o momento de investigarmos esta questão nevrálgica para o uso de IoT.

Neste capítulo, estudaremos algumas fragilidades clássicas considerando a necessária associação entre objetos IoT e sua conectividade. Nossa abordagem será construída de forma a evitarmos conceitos técnicos profundos de hardware e redes, por entendermos não serem estes os objetivos do presente estudo. Deixaremos, entretanto, indicadas as referências para o aprofundamento dos tópicos.

Ao final deste capítulo, você terá uma visão técnica geral de segurança para IoT, conhecendo suas incertezas e desafios. Conhecerá, também, o regramento legal que envolve a coleta de dados pessoais, por sensores ou não.

Vamos então dar início a este empolgante estudo com a revisão de alguns conceitos de segurança que subsidiarão o aprendizado de segurança voltado a IoT.

TEMA 1 – INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Após a metade do século passado, o mundo passou a conviver com facilidades de comunicação e, consequentemente, de troca de informações impossíveis de controlar. Este despertar assustador das telecomunicações estabeleceu um contraponto inusitado, em relação ao alto controle, que os Estados mantinham, sobre o tráfego de informações.

A popularização das máquinas computacionais e, posteriormente, de uma rede de interconexão acadêmica entre computadores, a internet, tornou informações restritas facilmente compartilháveis e, portanto, devassáveis. Os estudos da segurança da informação, no domínio da computação, surgem em resposta a esta instabilidade traduzida em ameaças aos Estados e empresas.

Sistemas móveis e computação em nuvem têm seu crescimento atrelado, atualmente, à correspondente evolução das soluções de segurança, o mesmo deverá ocorrer no futuro da IoT (Alves, 2021).

Neste tópico, vamos estudar alguns fundamentos de segurança da informação, que nos serão úteis para a compreensão das necessidades voltadas a objetos inteligentes e suas redes de atendimento.

1.1 Dados, Informação e Valor da Informação

Do ponto de vista leigo, informação tem um conceito inexato proveniente das percepções de nosso relacionamento com o mundo. Do ponto de vista da ciência da computação, entretanto, o conceito de informação é mais preciso.

Até aqui, tratamos, de forma diversa, dados e informações, mesmo sem tê-los conceituado. Provavelmente você observou que informações foram propositalmente elevadas a um patamar de valor superior aos dados brutos. Quando exemplificamos o uso de IA sobre dados coletados em sensores, comentamos que, após as fases de pré-tratamento e análise, os dados ganham o “status” de informação.

Podemos dizer que a depuração e tratamento dos dados coletados, no exemplo que comentamos, aporta valor a esses dados. De fato, uma informação, construída a partir da análise de dados é considerada um patrimônio, um bem com valor econômico que pode ser realizado, vendido.

Naturalmente, podemos pensar em informações com valores diferentes. Informações que podem ser obtidas facilmente tem baixo valor, já outras, cujo acesso é extremamente difícil, possuem valor elevado. Tome o exemplo de um relógio, saber as horas (que é a obtenção de informação a partir da leitura dos dados dos ponteiros) tem baixo valor, mas conhecer o projeto eletrônico do relógio possui valor mais alto.

A literatura habituou-se a classificar a informação segundo **três graus de sigilo: informações públicas, reservadas ou confidenciais.** O valor da informação cresce a cada transição entre esses graus.

Durante os processos de produção, manuseio, armazenamento, transporte e descarte (dito **ciclo de vida**), expõe-se a informação à perda, dano ou vazamento. A essas possibilidades chamaremos de *incidentes de comprometimento da informação*.

A partir da compreensão do conceito de valor da informação e da possibilidade de incidentes, podemos intuir de que trata o estudo da segurança da informação.

É fato que, quando a informação passa pelos processos que descrevemos acima, o fator humano tem forte influência sobre a maior ou menor exposição aos incidentes. Assim, podemos afirmar que manter a segurança das informações de uma determinada organização não depende apenas de subterfúgios técnicos construídos em SW ou HW, mas, principalmente, da implementação de controles, políticas, processos e procedimentos internos, constantemente monitorados quanto a sua eficiência (ABNT NBR ISO/IEC 27002:2103).

1.2 Característica da Informação Segura

Podemos considerar uma informação como segura quando algumas características são mantidas e controladas. A literatura enumera sete características da informação segura: **confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade (não repúdio), privacidade e auditabilidade,** destas sete, as três primeiras (confidencialidade, integridade e disponibilidade) são aquelas mais significativas para a segurança de dispositivos, enquanto, as demais, se referem, mais propriamente, a guarda de dados.

Vamos entender um pouco mais cada uma destas características aplicadas aos dados. Uma informação segura deve manter seu nível de confidencialidade por todo seu ciclo de vida, sem mudança em seu conteúdo (integridade e autenticidade). Deve estar disponível sempre que dela se necessite (disponibilidade), garantida a privacidade dos envolvidos nos dados originários bem como sua veracidade (não repúdio). O ciclo de vida da informação deve ser, ainda, em uma informação segura, auditável, de forma que sempre se possa verificar quais as pessoas ou processos envolvidos em cada fase do ciclo.

Conhecidos esses detalhamentos, podemos dizer que a segurança da informação visa manter as características da informação inalteradas durante todo seu ciclo de vida.

Quais seriam os motivos pelos quais essas características se alterariam? Como comentamos, podem ocorrer incidentes de comprometimento. Estes

incidentes podem ter várias motivações, procedimentos incorretos de manipulação ou por interesses escusos, são dois exemplos importantes. Vamos entender um pouco mais sobre esses incidentes a seguir.

1.3 Vulnerabilidade e Ameaça

Quando a informação é indevidamente exposta, dizemos que essa informação se encontra vulnerável. Assim, **vulnerabilidades** são fraquezas no tratamento da informação que podem gerar incidentes de comprometimento, ou seja, incidentes que alteram uma ou mais das características da informação segura.

De qualquer forma, a presença de uma vulnerabilidade não é suficiente para que o incidente ocorra. É necessário que um **agente** esteja presente, quando esse agente é capaz de explorar uma vulnerabilidade diz que há uma **ameaça** possível.

Uma ameaça não é sempre intencional. Suponha um canal de dados não redundante, pelo qual propaga-se informação sem controle de erros. Uma falha no canal é uma ameaça à segurança destes dados. A falha no canal pode ser causada por vários fatores aleatórios, inclusive por intempéries incontroláveis.

1.3 Risco

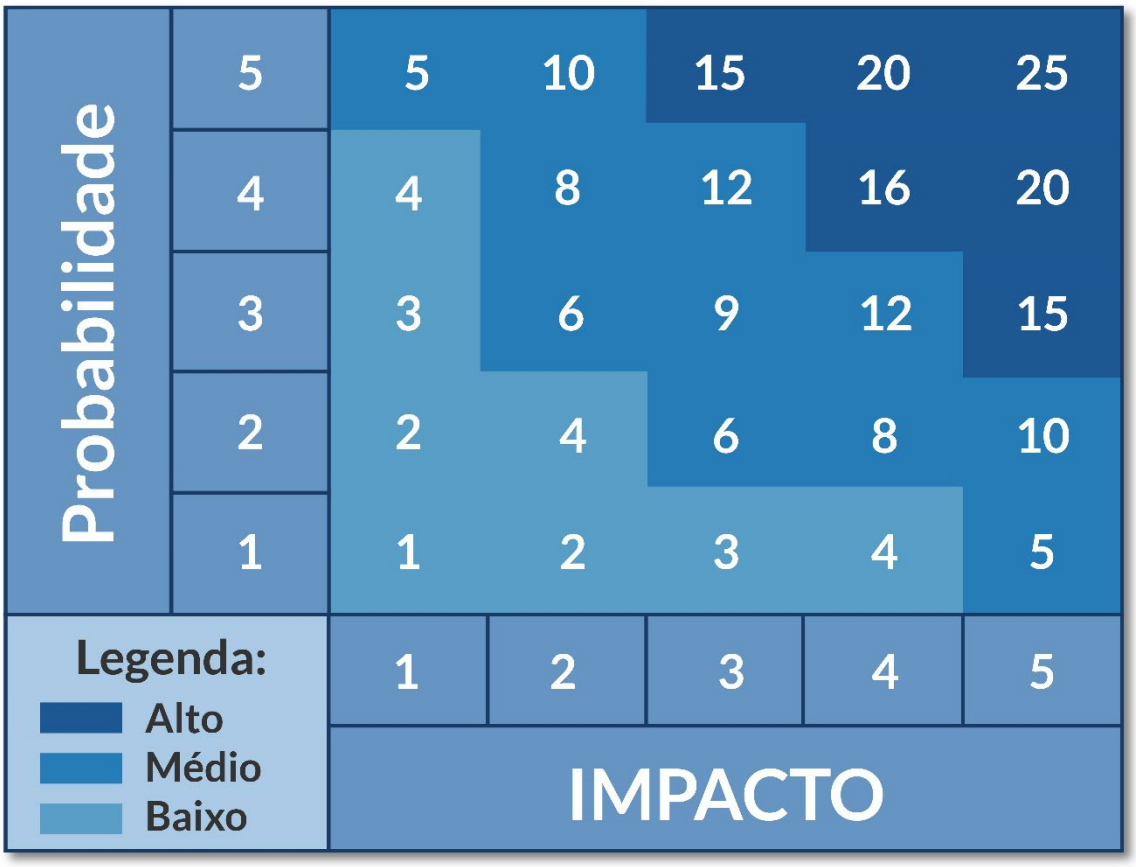
Presente uma ameaça e uma vulnerabilidade, existe o risco de que um incidente rompa as características da informação segura. Podemos pensar no risco como a probabilidade (estatística) de que uma ameaça obtenha sucesso em sua ação, mudando as características da informação.

Mesmo que uma ameaça gere um incidente, esse evento pode ter consequências, de diferentes graus, sobre a segurança de dada informação. Voltando ao exemplo de nosso canal, suponha que ocorra o colapso programado do canal, ao ser informada da futura interrupção, a equipe de operação pode encontrar uma alternativa para o tráfego das informações, tornando o impacto da ameaça baixo.

Desta forma, não basta conhecer as estatísticas de risco diante de um par ameça/vulnerabilidade, mas precisamos também estimar o impacto de cada risco sobre o negócio. A este processo denominamos gestão de risco. A figura a

seguir ilustra de que forma se estabelece uma análise quantitativa de riscos (PXI) a partir das estatísticas e estimativas citadas.

Figura 1 – Matriz de gestão quantitativa de risco



Fonte: ARTE:UT

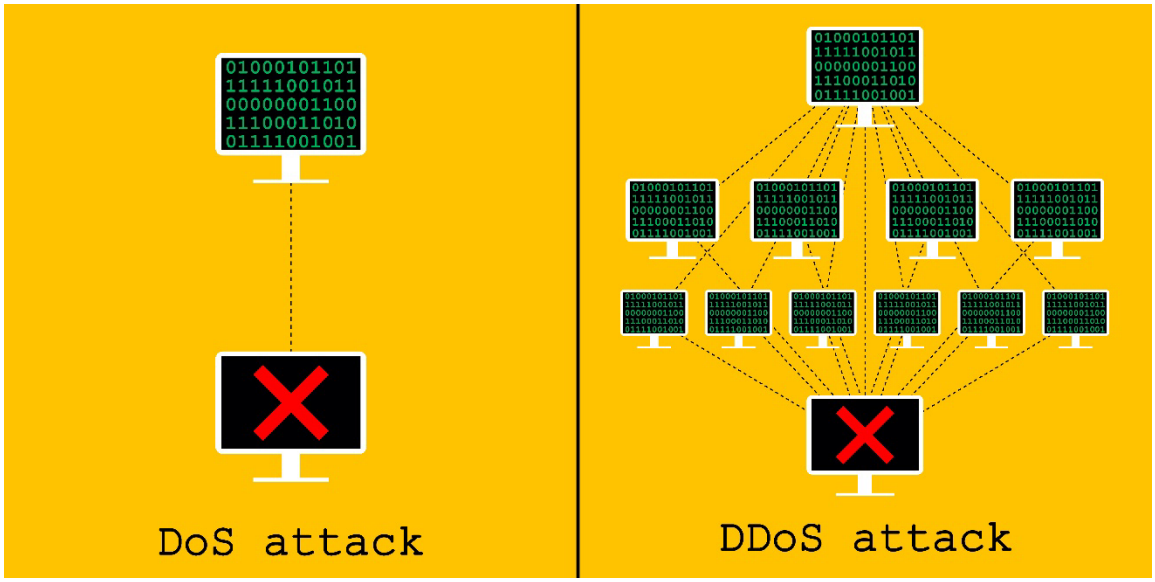
1.4 Ataques

Há, basicamente, dois tipos de ataques: passivos e ativos. Ataques ativos buscam alterar características dos dados. Essas alterações podem causar atuações indevidas, desligamentos, eliminação de dados, entre outras consequências. O ataque passivo, por sua vez, tem objetivo silencioso, de acessar indevidamente os dados, coletando informações reservadas ou confidenciais.

Ataque DoS e DDoS: Por ser o ataque mais expressivo em sistemas IoT, descreveremos brevemente essa modalidade de ataque ativo. DoS (Denial of Service, ou negação de serviço) e DDoS (DoS distribuído) são ataques típicos em redes conectadas à internet e têm por objetivo sobrecarregar o alvo com

inúmeras tentativas de conexão. A diferença entre a origem dos ataques DoS e DDoS ficam claras na figura a seguir.

Figura 2 – Origens DoS e DDoS



Créditos: nastasia Belic/Shutterstock.

As tentativas de conexão são propositalmente inválidas obrigando o alvo a negar cada solicitação de conexão. O esforço computacional para repudiar as conexões impede o alvo de tratar solicitações válidas.

Essa modalidade de ataque é bastante comum em sites comerciais de internet, causando a “queda” do site, bloqueando possibilidades de negócios hospedadas no endereço. Embora o objetivo de um ataque DoS seja sempre a retardar ou impedir o tráfego legítimo de rede, há três meios principais de ataque: ataque volumétrico, de protocolo e de aplicação.

O ataque volumétrico foca a camada de rede, normalmente explorando vulnerabilidade do protocolo UDP e ICMP. Ataques a protocolos visam esgotar a capacidade de processamento de ativos de rede como roteadores, servidores e firewalls. Estes ataques simulam pacotes de controle destes ativos, a exemplo do pacote de sincronização SYN, que exige resposta do alvo. Finalmente, os ataques à camada de aplicação inundam o HTTP com solicitações a uma determinada aplicação em um servidor (HTTP Flood), impedindo sua operação.

1.5 Contramedidas

Identificado um risco, cujo impacto pode ser importante, duas linhas de ação serão seguidas. Procedimentos técnicos são implementados para reduzir ao máximo a probabilidade de sucesso em um ataque (redução de risco). Considerando-se que, mesmo implementados tais procedimentos, o risco nunca será zerado e, portanto, sempre haverá a possibilidade de sucesso, mesmo que pequeno, em um ataque, um plano para minimizar o impacto, na eventualidade deste sucesso, precisa ser criado A estas técnicas de mitigação denominamos contramedidas. Podemos imaginar contramedidas que envolvam alterações de software (como gestão de senhas fortes), ou aquisição de firewalls, mas alterações de procedimentos que contornem vulnerabilidades ou controlem a possibilidade de se explorar uma vulnerabilidade (controle de acesso com segurança física, por exemplo) podem ser igualmente eficientes (Baars; Hintzbergen, 2018).

1.6 Triplo A

Ao se pensar em contramedidas, um bom balizador é o princípio do triplo A, acrônimo criado a partir as iniciais de autenticação, autorização e auditabilidade (*authentication, authorization, and accounting* em inglês). Segundo este princípio, toda informação, para ser acessada, precisa contar com um procedimento de autenticação. Este processo deve ser composto de ao menos duas, das três soluções de autenticação (autenticação por multifatores). A autenticação deve ser acompanhada de restrições de acesso, ou seja, o fato de se estar autenticado para determinado recurso não necessariamente garante acesso a todo o recurso. Finalmente, todas as manipulações feitas em uma informação precisam ser auditáveis, quanto à profundidade, tipo e autoria da manipulação.

1.7 DARPA

DARPA é a sigla da agência americana de pesquisa avançada em defesa (*Defense Advanced Research Projects Agency*, em inglês), criada em 1957, para manter os Estados Unidos à frente de estratégias de defesa cibernética.

A agência, além da pesquisa em vários campos da segurança tecnológica, publica recomendações e frameworks de segurança, principalmente

no que se refere a contramedidas de resposta a ameaças, com o objetivo de tornar o desenvolvimento de tecnologia, com fins lícitos, mais seguro.

As publicações de um de seus grupos de estudos, CERT, Computer Emergency Response Team, no mapeamento de ameaças, riscos e impactos, são especialmente interessantes para o estudo de segurança cibernética, servindo como balizador de estratégias de mitigação.

Os conceitos que apresentamos, de forma bastante sintética anteriormente, podem ser estudados com maior detalhamento em Galvão (2015), referenciado ao final deste capítulo.

TEMA 2 – ASPECTOS GERAIS DE SEGURANÇA PARA IoT

Após revisarmos a base de segurança da informação, vamos agora entender como esses princípios se adaptam a IoT, tanto no que se refere a dispositivos inteligentes quanto conectividade e camada de aplicação.

2.1 Confiabilidade, Integridade e Disponibilidade

Ao comentarmos as características da informação, enunciamos as sete principais, e observamos que as três primeiras têm aplicação em dispositivos computacionais de maneira geral. Dispositivos inteligentes não se constituem em uma exceção. Vamos então entender de que forma estas características se tornam objetivos para IoT.

A **confiabilidade** pode ser entendida como a necessidade de que dados transmitidos entre dois dispositivos cheguem ao destino e possam ser decodificados convenientemente. A implementação desse objetivo demanda, além de uma interface rádio eficiente, uma camada de controle de acesso ao meio com a complexidade necessária para recuperar a informação.

A **integridade** é a garantia de que estes dados serão recebidos com o exato conteúdo que foram transmitidos. Para que essa garantia esteja presente, deve-se impedir a adulteração da mensagem. No caso de ameaças maliciosas, métodos de criptografia coíbem a ação de hackers. O problema neste objetivo é a simplicidade do desenho de alguns objetos IoT. Parte dos dispositivos inteligentes priorizaram, em seu projeto, a redução de dimensões e custos,

deixando as implementações de segurança para uma camada superior, a critério do usuário (Popscul; Genete, 2016, p. 30).

A **disponibilidade**, por sua vez, pode ser implementada pela escolha de interfaces físicas que utilizem modelos de modulação resilientes e por métodos de controle e correção de erros, que garantam a resiliência da comunicação, frente às ameaças naturais e não intencionais.

Na sequência de nosso estudo, veremos a relação entre as características estudadas e as camadas IoT-A no modelo genérico, visto no início de nosso estudo.

2.2 Segurança na Camada de Percepção

Já ficou evidente, neste ponto de nosso estudo, que objetos inteligentes sofrem com fortes limitações de hardware, a exemplo de disponibilidade de energia, capacidade de processamento e memória limitada. As restrições de HW implicam em limitações de software, impedindo implementações complexas, entre elas aquelas voltadas a segurança. Apesar dessas limitações, as exigências em torno da IoT são altas, alguns exemplos são mobilidade, tamanho, escalabilidade, redes multiprotocolo e topologia dinâmica de rede (Popscul; Genete, 2016, p. 30). A combinação entre limitações do objeto e alta exigência de desempenho resultam em uma ampla variedade de vulnerabilidades potenciais.

Consideradas essas vulnerabilidades, imagine um smart space, a exemplo de um prédio inteligente, onde vários objetos inteligentes são combinados para extrair informações pessoais de seus habitantes, como suas características pessoais, movimentos, localização e atividades. Esses dispositivos podem ser ainda combinados com sensores “vestíveis” pertencentes à PAN (*Personal Area Network*), a exemplo de sensores de temperatura corporal e ritmo cardíaco. O potencial de impacto, de acesso indevido a estes bases de dados, é alto.

As ameaças não envolvem apenas sensores inteligentes, atuadores inteligentes estão presentes nesses ambientes e uma infecção tem o potencial de gerar a perda de controle sobre dispositivos de restrição de acesso, veículos inteligentes, provimento de energia, água etc. Essas ameaças não são apenas hipotéticas. O risco foi comprovado pelo colapso provocado por ataque cibernético na rede automatizada de distribuição de energia elétrica da Ucrânia

em 2015, que deixou cidades inteiras no escuro, por bom tempo (Syed *et al*., 2021, p. 458).

De maneira geral, podemos dizer que a camada de percepção pode estar vulnerável a ataques que danifiquem a estrutura de hardware, de software, ou ambas.

As vulnerabilidades de hardware podem ser físicas ou lógicas, a exemplo de alterações danosas de configuração ou danos diretos ao hardware instalado.

Os ataques ao software do dispositivo podem ser tanto ativos quanto passivos. No primeiro caso, o comprometimento do acesso (alteração de senhas) ou a destruição da estrutura do sistema operacional, constituem-se em exemplos de ataque. A escuta, ou captação de dados, nos dispositivos é exemplo de ataque passivo de software.

Vulnerabilidade no SO: neste ponto, devemos comentar sobre uma vulnerabilidade relacionada ao SO de alguns objetos. Quando descrevemos os SOs, usados em IoT, comentamos que entre os mais frequentes estão Contiki e Tiny, ambos desenvolvidos em C.

A linguagem C, por ser mais rústica em relação às linguagens atuais, não possui, nativamente, certas facilidades de consistência da programação, com as quais estamos acostumados na programação contemporânea. Um exemplo, bastante citado na literatura, são os estouros de estruturas de dados. Definida uma estrutura qualquer, se durante a operação ultrapassarmos os limites definidos em sua criação, o programa se perderá, considerando valores armazenados nas posições próximas de memória como pertencentes à estrutura. O mesmo se dá em relação a definição de variáveis e ponteiros. As posições de memória alocadas permanecem com os valores lá residentes se não as inicializarmos convenientemente.

Programadores C experientes, conhecendo essas fragilidades ligadas à própria simplicidade da linguagem, implementam códigos padrão de contorno. Como esse uso não é frequente na programação recente, APIs customizadas tendem a apresentar estas vulnerabilidades clássicas.

Ataques que exploram tais vulnerabilidades se assemelham aos de negação de serviço (DoS), mas buscam forçar o objeto a execução de requisições válidas em grande quantidade, de forma a explorar eventuais limites não protegidos, das estruturas de dados.

2.3 Segurança na Camada de Rede

Redes de objetos IoT são normalmente pouco seguras, porque as implementações de segurança clássicas são “pesadas” em demasia, para o processamento destes objetos mais simples. Isso torna o uso de um protocolo seguro de redes como IPsec, por exemplo, inviável para IoT.

As soluções para a segurança de rede ainda são parcas e deixadas a cargo das camadas inferiores, com a inserção de processos de criptografia de dados na camada MAC. O acréscimo de facilidades de autenticação na camada de aplicação é outra estratégia possível. Comentaremos mais a respeito dessas limitações ainda neste capítulo.

2.4 Segurança e Aplicação

A defesa de uma aplicação de controle em IoT não difere, do ponto de vista essencial, daquela estudada para qualquer outro tipo de aplicação de nuvem. A grande vicissitude está na amplitude da superfície de ataque e no alto impacto do acesso indevido a dados pessoais. Esse duplo aspecto do risco, técnico por um lado (relacionado a superfície de ataque) e jurídico por outro, será objeto de aprofundamento em nossos próximos tópicos.

Quando uma série de objetos IoT são direcionados e tratados, em uma única plataforma, a possibilidade de se produzir uma vulnerabilidade é alta. Se essa concentração ocorre em ambiente interno de uma corporação, contramedidas podem ser desenhadas de forma a blindar o acesso externo à plataforma e controlar o acesso interno pelo uso de procedimentos de segurança AAA.

A questão se torna realmente problemática quando tratamos de cidades inteligentes. Nesse caso, os objetos e subredes não são amistosas entre si e a concentração das informações na plataforma pública também significa concentração de ameaças. Há dois aspectos a serem analisados nesse ponto.

Por um lado, defender os dados de nuvem, abrigados em um data center, depende do estabelecimento de uma série de barreiras técnicas à invasão implementáveis pelo gestor do data center.

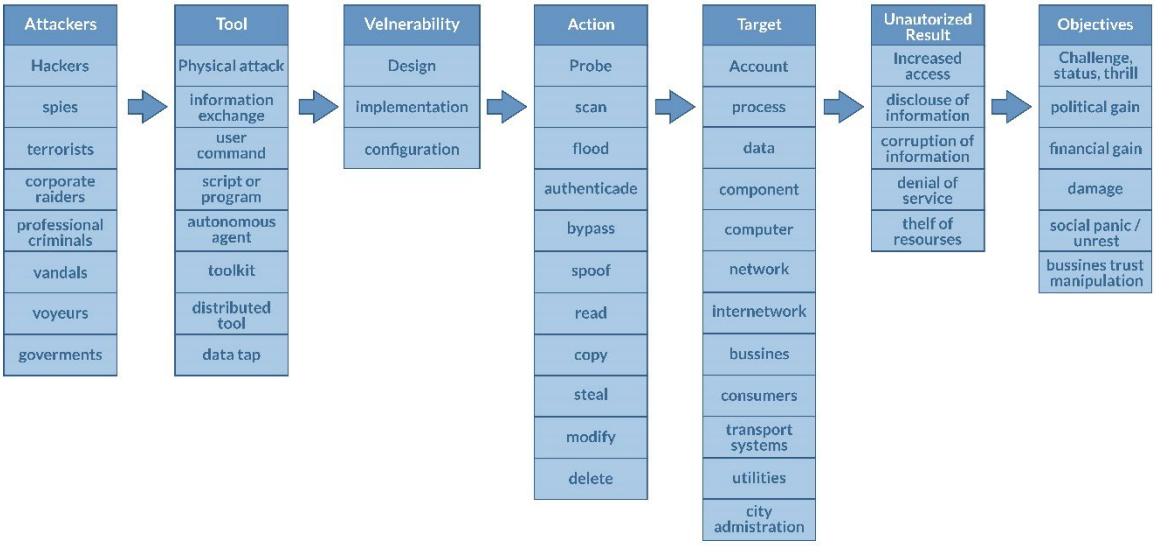
Por outro lado, considerando que o acesso indevido aos dados, apesar de todas as defesas técnicas, poderá ocorrer em algum momento, é necessário que os dados sejam armazenados cumprindo critérios criptográficos estritos.

Cabe à administração municipal e as empresas manipuladoras dos dados, os cuidados com este segundo nível de segurança, que além de implementar medidas de preservação das sete características da informação segura de maneira geral, dará a especial ênfase à privacidade e confidencialidade. Esse destaque precisa ser estudado frente às sanções previstas nas legislações de proteção de dados presentes na maioria das nações. São exemplos dessas regulamentações legais a GDPR (General Data Protection Regulation ou Regulamento Geral de Proteção de Dados) em vigor desde 2018 no continente europeu e a Lei 13.709 (Lei Geral de Proteção de Dados) no Brasil, a esses temas voltaremos ainda neste capítulo.

2.5 Vulnerabilidades e Riscos em IoT

A identificação das vulnerabilidades e riscos consequentes, não difere, do ponto de vista genérico, dos presentes em outras tecnologias computacionais. O diagrama da figura abaixo adapta o estudo de identificação da DARPA para IoT.

Figura 3 – Taxonomia de ameaças cibernéticas proposta pelo CERT para IoT



Créditos: SYED *et al.*, 2021, p. 460.

Observe que, além das vulnerabilidades inerentes das redes IoT, existem outras, provenientes tanto de equívocos de configuração, quanto de implementação. Dito de outra forma, não apenas as vulnerabilidades próprias da tecnologia, que estudamos neste capítulo, são responsáveis pelos riscos de segurança, mas também questões de projeto e operação. Esta não é uma novidade propriamente, projetos e operação indevida são imputáveis por boa

parte das invasões cibernéticas. A baixa maturidade da tecnologia IoT, entretanto, torna a existência destas vulnerabilidades mais provável.

TEMA 3 – PRIVACIDADE E IoT

Quando comentamos sobre os riscos envolvendo a camada de aplicação, dividimos os riscos em técnicos, principalmente envolvendo os protocolos de comunicação e questões jurídicas, causadas pela eventual quebra de privacidade de dados.

Este segundo enfoque ganha bastante importância frente as exigências de nosso ordenamento jurídico. Neste tópico, vamos conhecer um pouco destas exigências e do possível impacto envolvido no uso da tecnologia IoT.

3.1 Noções de Direito

Para que possamos corretamente localizar a legislação que rege a privacidade de dados, é necessário que entendamos alguns rudimentos de Direito.

A sociedade humana sempre enfrentou o problema do comportamento inadequado de alguns indivíduos de uma forma relativamente simples, delegando ao líder tribal e posteriormente ao nobre ou ao rei a autoridade para determinar a punição a este membro.

O problema que surge, desta delegação ilimitada de poder, é falta de garantia da equanimidade das decisões envolvendo comportamentos semelhantes. Maior era o problema quando o próprio nobre apresentava atitudes reprováveis pela sociedade. Sem limites aceitos por todos, inclusive pelos detentores do poder, não poderia haver justiça efetiva.

Os romanos foram os primeiros a concretizar uma coletânea organizada de regras (*lex* em latim) de comportamento, que estabeleciam formas padrão para relacionamentos comerciais, afetivos e entre castas sociais. A sociedade medieval recuou na padronização das regras, mas diante de abusos da monarquia inglesa a ideia de limitar o poder dos nobres renasceu. Surge assim a primeira Constituição que teve por objetivo (como ainda o tem) limitar o poder do líder, estabelecendo os direitos básicos dos liderados.

A Constituição é o regramento máximo de uma nação. Nela se pode estabelecer quais as restrições de direitos aceitáveis e qual o meio de concretiza-

las. A Constituição brasileira estabelece que o detalhamento e aplicação das regras constitucionais seja feito pelas leis complementares e, abaixo destas, pelas leis ordinárias federais como formas de regrar o comportamento dos cidadãos (Art.5º., II, CF). Há, portanto, uma hierarquia vinculante entre as leis, não pode haver lei que se contraponha aos ditames constitucionais, assim como não haverá lei estadual ou municipal que desrespeite o estabelecido em lei federal. Essas contradições, se ocorrerem, invalidam a lei que as perpetua, parcial ou totalmente, sem que seja necessária qualquer ação do cidadão.

No que se refere à proteção da privacidade de dados, no Brasil, a lei ordinária federal 13.709, de 14 de agosto de 2018, acunhada Lei Geral de Proteção de Dados Pessoais (LGPD), é a responsável por regrar o uso dos dados pessoais obtidos dos cidadãos brasileiros.

3.2 LGPD

Como já sabemos, a LGPD estabelece limites à coleta e utilização de dados pessoais no Brasil. Essa lei é uma resposta de nossos legisladores a um movimento mundial de preservação da privacidade, por meios legais, diante da enorme disponibilidade de dados cibernéticos, cuja divulgação perturbaria o direito à privacidade.

A LGPD, em seu art. 2º., enumera os fundamentos da proteção de dados pessoais, citemos, entre os lá descritos, o respeito à privacidade, à liberdade de expressão, de informação, de comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem. Diante desses fundamentos, a lei vincula a coleta e uso de dados pessoais ao consentimento livre, informado e inequívoco, desde que expressamente utilizados para uma finalidade determinada.

Não só o consentimento é exigido pela lei, mas, em seu art. 9º, há também a necessidade de que o cidadão tenha acesso livre e facilitado ao tratamento de seus dados, permitindo-se, a qualquer tempo, a reversão do consentimento.

Outro direito importante se refere à anonimização de dados sensíveis (Cap.II, Seção II), ou seja, dados que podem expor aspectos indesejados pelo cidadão devem perder a capacidade de identificação de sua origem.

Finalmente, o art. 46 imputa a aqueles que coletarem dados, a adoção de medidas de segurança, técnicas e administrativas, de forma a evitar acessos não autorizados e destruição, perda ou alteração dos dados originais ou tratados. Estabelece, ainda, o art. 50, que regras de boas práticas, de governança e

mecanismos internos de supervisão e de mitigação de riscos, sejam compulsoriamente implementados pelos operadores de dados pessoais. A quebra desses institutos legais gera direito à indenização cível e reparação penal.

3.3 LGPD e IoT

Como discutimos, há severas limitações à coleta de dados inadvertidos assim como (e principalmente) à abertura de dados sensíveis para terceiros não expressamente autorizada.

Os dados coletados por sensores IoT podem pertencer à categoria de dados anônimos, quando coletados com objetivos estatísticos, neste caso deve haver garantia de anonimização, que impeça a conexão entre o dado e o indivíduo. Há, entretanto, principalmente em cidades inteligentes, coleções de dados não anônimos disponíveis.

Como entendemos pelo estudo da LGPD, os dados fazem parte do patrimônio privado individual e, por tal motivo, não podem ser coletados sem a autorização expressa, derrogável e com propósito definido. Há aqui uma discussão possível sobre essa coleta inadvertida de dados, ou seja, ao coletarmos os dados de um cartão de transporte, por exemplo, ele será obrigatoriamente não anônimo e revelará informações sobre os hábitos de seu proprietário, não autorizadas a priori. Essas informações, então, precisam ser descartadas com segurança ou anonimizadas, se forem utilizadas para uso estatístico. A lei exigirá, sob pena de indenização, que esse processo seja auditável.

Até este ponto, entretanto, o problema é controlável. A questão crucial surge quando o sistema de coleta, armazenamento ou tratamento, que apresenta vulnerabilidades, como já estudamos, for devassado.

Os custos de implementação de contramedidas são facilmente suplantáveis pela necessária resposta judicial a esta quebra de exigência do instituto legal. Essa realidade obrigará, a todas as empresas envolvidas no fornecimento de serviços inteligentes, a fortes investimentos em segurança e a constantes avaliações de risco.

TEMA 4 – SEGURANÇA EM MQTT

Como comentamos anteriormente, além do enfoque legal, há um fator de risco de alto impacto para a segurança de objetos IoT, relacionado aos protocolos, principalmente na comunicação entre camadas de aplicação. Vamos, a seguir, conhecer algumas fragilidades do protocolo mais usados nessa camada, o MQTT, apresentado em outro momento.

4.1 Vulnerabilidades

O protocolo MQTT e suas implementações, como o servidor Mosquitto, possuem foco na dimensão de disponibilidade e menor em integridade e confiabilidade. Esse fato está ligado às limitações da própria tecnologia, como já elucidamos. Dessa forma, o MQTT não implementa, nativamente, processos fortes de autenticação das entidades conectadas ao servidor nem de criptografia.

A ausência de autenticação resiliente permite a entrada de entidades espúrias na rede, aceitas como sensores/atuadores válidos. Essa entrada de espúrios, associadas a ataques de DoS nos sensores válidos, resultam em contaminação das informações disponíveis no servidor.

A ausência de criptografia fim a fim, por sua vez, permite o vazamento por ataque passivo e facilita a operação de contaminação que descrevemos acima, uma vez que os dados circulam no meio, sem que uma senha os proteja tanto de leitura quanto de escrita indevida.

Os protocolos de camadas inferiores, dependendo da seleção de padrão, como já estudamos, podem garantir a integridade dos pacotes de dados, inclusive criptografando-os. Como a criptografia provida pelas interfaces de rede é aberta para o protocolo MAC, o uso de uma mesma interface tornará o processo transparente, retirando a garantia da comunicação fim a fim da camada de aplicação.

A implementação de segurança de rede, como SSL/TLS, clássica contramedida para DoS, se vê impedida pela restrita capacidade de processamento dos dispositivos além do overhead inevitável nos pacotes.

4.2 Métodos de Hash

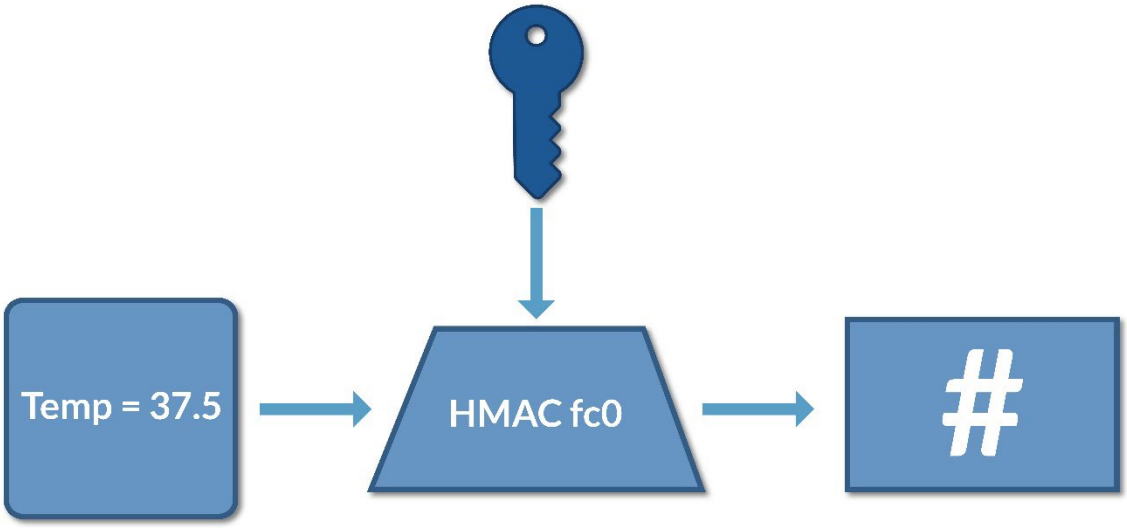
Uma solução que leva em conta as limitações dos dispositivos, é a criação de Hash. Um hash é um código de autenticidade da mensagem, que é

transmitido em algum ponto negociado entre cliente e servidor da comunicação. Normalmente são cálculos matemáticos simples como a soma de checagem (checksum) de baixa exigência computacional.

Esses métodos, embora rápidos e simples, podem garantir a integridade da mensagem, mas não atuam sobre a confiabilidade. Um ataque que vise alterar o conteúdo seria detectado, por essa técnica, mas um dispositivo espúrio, após obter seu registro na rede, pode mandar mensagens maliciosas desde que conheça o hash. O problema é que os métodos de hash são públicos e padronizados.

Há, entretanto, uma alternativa interessante, pelo uso de HMAC (**keyed-hash message authentication code**) ou código de autenticação de mensagem com chave hash. Nesse caso, a geração do Hash combina o cálculo matemático da mensagem com uma chave ou senha, conforme representado a seguir, para um sensor de temperatura.

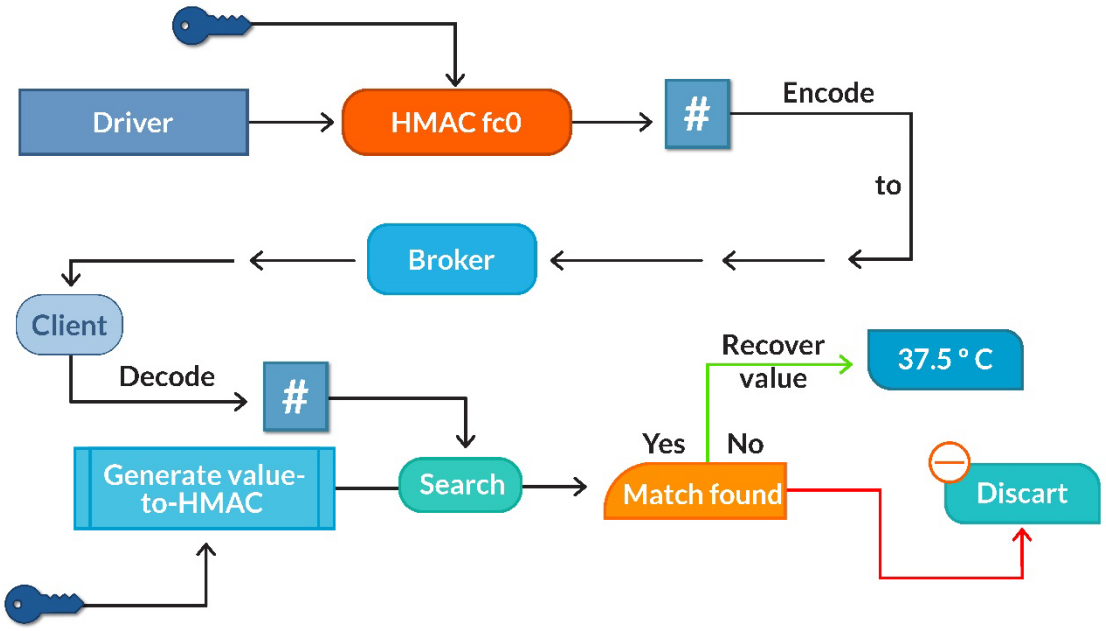
Figura 4 – Implementação de HMAC



Fonte: Dinculeană *et al*., 2019.

Essa solução implica a necessidade de troca de uma chave entre dispositivo e servidor, se confinarmos a segurança entre estes. É possível, entretanto, estender a segurança em direção ao assinante final, permitindo a ele a verificação de autenticidade da informação. Nesse caso, a troca de chaves precisa envolver também a estes últimos. A figura a seguir ilustra o processo fim a fim.

Figura 5 – Implementação de HMAC fim a fim



Créditos: Dinculeană *et al.*, 2019, p. 7.

A distribuição da chave constitui-se em um novo problema a ser enfrentado. Também deve-se comentar que, superada a dificuldade no compartilhamento da chave, a estratégia HMAC contorna o problema da confiabilidade, mas não atua sobre a contenção de um ataque de negação de serviço.

Distribuição de Chave Criptográfica: como acabamos de comentar, soluções de hash podem ser bastante eficientes, mas a distribuição da chave é uma questão em aberto. Estratégias clássicas (não voltadas a IoT) tendem a utilizar chaves assimétricas. Nessa aproximação, distribui-se uma chave pública para encriptação, mas mantêm-se a chave privada confidencial. Desta forma, é possível a entrada de um novo dispositivo na rede sem quebra da segurança criptográfica. Chaves assimétricas, entretanto, exigem capacidade computacional para a implementação dos complexos algoritmos matemáticos envolvidos. Segundo Simplício *et al*. (2010), cuja leitura indicamos para aprofundamento deste tópico, a memória de um objeto IoT, rodando algoritmos assimétricos, é comprometida em até 90%, impedindo sua escolha para esta tecnologia.

Métodos de chave simétrica são rápidos e demandam computação aceitável para IoT, mas, por compartilhar uma única chave de encriptação e

decriptação, pode ter a segurança da rede comprometida no momento de entrada de um novo dispositivo, que exigirá a divulgação da chave.

A solução estudada por Simplício *et al*. (2010) é a pré-distribuição de chave. Desta forma, o objeto novo sofrerá um login inicial, em uma entidade confiável, encarregada do pré set dos dispositivos.

4.3 Predição de Ataque

Uma outra solução, que agrada a parte da comunidade científica, está ligada ao uso de processos de predição de anomalias na camada de percepção. Esta contramedida opera na origem da ameaça, identificando o ataque DoS.

Tentativas de bloqueio dessa modalidade de ataque esbarram na identificação da origem. Para que se detecte o DoS é necessário que seja possível distinguir um assinante malicioso daquele legítimo. Em aplicações voltadas à internet, de maneira geral, esta percepção é bastante difícil e passa por atualização constante de listas negras e brancas do firewall (ACLs).

Na solução proposta para IoT, buscou-se reproduzir um pequeno IDS (*Intrusion Detection System* ou sistema de detecção de invasão), residente no servidor próximo, evitando sobrecarga de processamento dos dispositivos. Para que não seja necessária a geração de ACLs a solução baseia-se em IA e análise estatística.

O tráfego de rede, no lado dos publicadores, é analisado em condições de ataque zero, gerando uma base de comparação. O mesmo processo estatístico pode ser aplicado ao lado assinante, evitando ataques provenientes da internet. Cria-se, então, uma camada de segurança, antecessora da aceitação de solicitações MQTT, no servidor. Se o tráfego nos publicadores ou assinantes for anômalo, a solicitação não é enviada para processamento do Broker. Maiores detalhes sobre uma implementação desta solução podem ser encontrados no artigo de AP *et al*. (2019).

TEMA 5 – SEGURANÇA EM MODELOS COMPUTACIONAIS FOG E EDGE

Objetos IoT podem ter capacidades computacionais bastante diversas em função da aplicação para a qual foram desenvolvidos. Como já sabemos, a grande maioria das soluções de IoT, por questões econômicas, focam em objetos de baixíssima capacidade computacional. Fato é que essa simplificação

extrema, em alguns casos se transforma em problema, na mesma direção em que tentou ser uma solução. A exigência de processamento centralizado, em nuvem, cresce exponencialmente, quando a quantidade de dispositivos elementares se eleva.

Diante do congestionamento no serviço de nuvem, soluções de processamento distribuído foram necessárias, devolvendo a ponta a capacidade de processamento que inicialmente lhe fora negada. Como já estudamos, há dois modelos de distribuição de processamento em IoT: Fog e Edge. Vamos agora entender como o que estudamos sobre segurança até o momento se adapta a estes modelos distribuídos.

5.1 Segurança em Neblina (Fog)

O modelo de computação de neblina é um passo intermediário a devolução da capacidade de processamento para os dispositivos. Nessa arquitetura, a rede local de percepção se vê confinada em relação à WAN ou internet pelo concentrador. Desta forma, do ponto de vista de segurança, o problema se vê dividido.

Parte da rede, entre concentrador e servidor de nuvem, se torna clássica. Trata-se de uma rede de máquinas computacionais e não mais de uma rede de objetos IoT, a ser protegida.

A segunda parte, entre concentrador e objetos, está isolada e o concentrador pode implementar contramedidas de firewall. As ameaças internas são controláveis, uma vez que o concentrador conhece os objetos a ele conectados ou conectáveis.

5.2 Segurança em Borda (Edge)

O modelo de computação de borda é um passo final de devolução da capacidade de processamento para os dispositivos. Como já discutimos, o tempo de processamento de soluções envolvendo decisão centralizada pode ser problemático para determinadas aplicações, principalmente em cidades inteligentes, motivando a devolução de parte do processamento para a borda.

Do ponto de vista de segurança, as mesmas observações feitas sobre Fog podem ser aqui repetidas. O problema se vê dividido. Naturalmente, essa divisão permite maior foco nas estratégias de contramedidas em cada nível de

computação. Além disso, a crescente capacidade de processamento em cada nível faculta a implementação de estratégias clássicas de debelamento de ataques.

FINALIZANDO

Neste capítulo, buscamos examinar os desafios ligados à segurança de serviços, que utilizam camadas sensoriais IoT. São dois aspectos, igualmente importantes, na definição dos protocolos de análise de risco X impacto e na escolha de contramedidas. O aspecto técnico está, ainda, como a própria tecnologia IoT, em fase de pesquisa, sem soluções sedimentadas disponíveis. O aspecto legal, que estabelece responsabilidade subjetiva aos operadores de dados, aporta apelo aos investimentos em soluções de proteção de dados e garantia de anonimização. Essa combinação gera forte preocupação com a segurança desses objetos, redes e aplicações.

Ao concluirmos este estudo, entendemos que certa frustração resta proveniente da impossibilidade de se oferecer certezas e métodos eficientes e consolidados em relação ao universo IoT. Certamente apresentamos, por outro lado, francos indícios de tecnologias que podem, com a devida evolução, prover as soluções necessárias.

Para aqueles que pretendem dedicar-se a essa ainda lacunosa área de estudo, recomendamos a leitura dos artigos referenciados ao final, escolhidos de forma a contemplar autores e entidades importantes na definição do futuro da tecnologia IoT e, posteriormente, acompanharem as publicações a eles relacionadas.

REFERÊNCIAS

AP, H. *et al*. Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. **EURASIP Journal on Wireless Communications and Networking**, n. 1, p. 1-15, 2019.

ALVES, D. **Internet das Coisas (IoT)**: Segurança e Privacidade de Dados Pessoais. Rio de Janeiro: Alta Books, 2021.

BAARS, H.; HINTZBERGEN, K.; HINTZBERGEN, J. **Foundations of Information Security**: based on ISO 27001 and 27002. Rio de Janeiro: Brasport, 2018.

BAR-MAGEN, J. Fog computing: introduction to a new cloud evolution. In: **Escrituras silenciadas**: paisaje como historiografía. Editorial Universidad de Alcalá, 2013. p. 111-126.

DE PAULO, W. L.; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. **Revista Contabilidade e Finanças**, v. 18, n. 43, USP, São Paulo, jan./abr. 2007.

DINCULEANĂ, D.; CHENG, X. Vulnerabilities and limitations of MQTT protocol used between IoT devices. **Applied Sciences**, v. 9, n. 5, p. 848, 2019.

GALVÃO, M. da C. **Fundamentos em segurança da informação**. São Paulo: Pearson Education, 2015.

POPESCUL, D.; GENETE, L.-D. Data security in smart cities: challenges and solutions. **Informatica Economică**, v. 20, n. 1, 2016.

SIMPLÍCIO JR, M. A. *et al*. A survey on key management mechanisms for distributed wireless sensor networks. **Computer networks**, v. 54, n. 15, p. 2591-2612, 2010.

SYED, A. S. *et al*. IoT in smart cities: a survey of technologies, practices and challenges. **Smart Cities**, v. 4, n. 2, p. 429-475, 2021.