Introdução à Internet das Coisas

Segurança e Privacidade

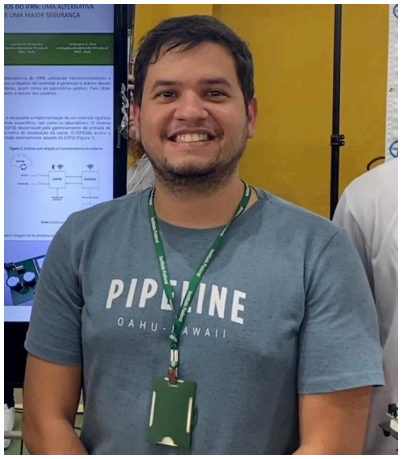
Apostila do aluno

Ph.D. Andouglas Gonçalves da Silva Júnior
Ph.D. Manoel do Bonfim Lins de Aquino
Marcos Fábio Carneiro e Silva
Autor da apostila

Ph.D. Andouglas Gonçalves da Silva Júnior
Ph.D. Manoel do Bonfim Lins de Aquino
Instrutor do curso

Larissa Jéssica Alves – Analista de Suporte Pedagógico
Revisão da apostila

Autor



Andouglas Gonçalves da Silva Júnior

Doutor em Engenharia Elétrica e da Computação - UFRN. Mestre em Engenharia Mecatrônica na área de Sistemas Mecatrônicos. Bacharel em Ciências e Tecnologia pela EC&T - Escola de Ciências e Tecnologia - UFRN. Engenheiro Mecatrônico - UFRN. Professor de Ensino Básico, Técnico e Tecnológico no Instituto Federal de Educação Tecnológica do Rio Grande do Norte (IFRN). Integrante da Rede de Laboratórios NatalNet, LAICA e colaborador ISASI-CNR-Itália. Desenvolve projetos na área de Machine Learning, Internet das Coisas e Holografia Digital. Colabora no projeto do N-Boat (Veleiro Robótico Autônomo), principalmente no desenvolvimento de sistemas para monitoramento da qualidade da água e identificação de micropartículas usando holografia digital e IA.

Manoel do Bonfim Lins de Aquino

Possui graduação (2006), mestrado (2008) e doutorado (2022) em Engenharia Elétrica e da Computação, pela Universidade Federal do Rio Grande do Norte - UFRN. Tem experiência na área de projetos de Telecomunicações, atuando na Siemens como engenheiro de Telecomunicações (2008-2010). Sou Professor (2010 - atual) do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - IFRN, membro do NADIC, Núcleo de Análise de Dados e Inteligência Computacional, onde venho desenvolvendo projetos de P&D nas áreas de desenvolvimento de sistemas, IoT e Inteligência Artificial.

Marcos Fábio Carneiro e Silva

Estudante de informática no Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte. Participou, como bolsista, de projeto de pesquisa voltado à automação em ambiente escolar com IoT (2022 - 2023), Possui experiência em redes de computadores, eletrônica e IoT, com ênfase na utilização de microcontroladores e desenvolvimento de Hardware. Além disso, possui conhecimentos básicos em Python e C++. Atualmente é membro do NADIC (Núcleo de Análise de Dados e Inteligência Computacional) do IFRN.

APRESENTAÇÃO

Bem-vindo ao curso de **Introdução à Internet das Coisas** do *CEPEDI!*

A Internet das Coisas, ou IoT, é uma revolução tecnológica que está transformando a maneira como interagimos com o mundo ao nosso redor. Essa inovadora e crescente rede de dispositivos interconectados, que variam desde sensores e aparelhos domésticos até veículos e equipamentos industriais, está desencadeando uma mudança fundamental em como coletamos, compartilhamos e utilizamos informações.

Neste curso, introduziremos o fascinante mundo da IoT, definindo conceitos básicos, seus principais componentes e aplicações. Além disso, introduziremos os protocolos de comunicação mais usados em aplicações de Internet das Coisas, além dos principais dispositivos utilizados hoje, como ESP32, Arduino, Raspberry Pi Pico, entre outros.

Além disso, pretendemos oferecer um curso que mescle a teoria com a prática. Para isso, utilizaremos aplicações livres como Wokwi e Bipes para desenvolvimento de projetos que nos auxiliarão no aprendizado dos conceitos teóricos.

Recomendamos ao aluno que, ao final da leitura de cada seção, realize os exercícios propostos e acesse os materiais indicados nas referências bibliográficas, para aprofundar a leitura desse material e complementar o que foi lido aqui.

Desejo a você, prezado aluno, que tenha um excelente curso!!

Boa Leitura !!

Sumário

1 Segurança e Privacidade em IoT

A segurança e privacidade na era da Internet das Coisas (IoT) são temas de extrema importância devido às vastas oportunidades econômicas e inovações que essa tecnologia proporciona em setores cruciais como saúde, energia, fabricação e transporte. Enquanto as soluções e empresas buscam colher os benefícios da IoT, enfrentam desafios significativos relacionados à segurança cibernética, privacidade e conformidade.

A segurança tradicional cibernética concentra-se predominantemente no software, mas a segurança de IoT acrescenta complexidade ao abranger a convergência do mundo cibernético e físico. A conectividade de dispositivos torna-se crucial, destacando a importância de padrões de segurança para prevenir violações, desastres e ameaças.

1.1 Riscos e ataques à IoT

Embora muitos dispositivos de IoT possam parecer inofensivos, eles estão suscetíveis a serem sequestrados, resultando em espionagem, interrupção de serviços e até mesmo crimes cibernéticos. Estes ataques podem comprometer não apenas a segurança digital, mas também a infraestrutura física, causando danos operacionais e físicos.

Os ataques à IoT abrangem uma gama diversificada, incluindo falsificação, adulteração, divulgação de informações confidenciais, negação de serviço e elevação de privilégios. Eles podem afetar tanto os **processos** da aplicação, bem como a **comunicação** e/ou **armazenamento**. Exemplos práticos incluem:

- **Falsificação:** Envolve a falsificação de dados ou mensagens para enganar dispositivos ou sistemas IoT. Exemplos incluem falsificação de identidade de dispositivo e falsificação de dados de sensor.
- **Adulteração:** Envolve a modificação de dados ou software em dispositivos IoT, como ataque de malware ou ataque de firmware.
- **Divulgação de informações confidenciais:** Envolvem o acesso não autorizado a dados confidenciais armazenados em dispositivos ou sistemas IoT, como ataque de espionagem ou interceptação.

- **Negação de Serviço (DoS):** Envolve a sobrecarga de dispositivos ou sistemas IoT com tráfego falso, tornando-os indisponíveis para usuários legítimos. Exemplos incluem ataque DoS volumétrico e ataque DoS de baixo e lento.
- **Elevação de privilégio:** Envolve a obtenção de acesso não autorizado a um nível mais alto de privilégio em um dispositivo ou sistema IoT, como ataque de escalada de privilégios ou ataque de força bruta.

1.2 Segurança em Camadas

De forma a facilitar a divisão das diferentes formas de segurança que podemos aplicar em soluções IoT, vamos analisar cada camada separadamente, indicando como podemos evitar diferentes ameaças que podemos encontrar nas aplicações práticas de IoT.

Camada de Percepção

A camada de Percepção envolve dispositivos que coletam informações e recebem comandos dos usuários. Ela representa uma das camadas mais sensíveis na arquitetura da Internet das Coisas (IoT). Por isso, golpistas realizam uma série de ataques distintos visando obter controle sobre esses dispositivos e acessar os dados coletados por eles. A seguir, apresentamos as ameaças mais comuns desta camada.

- **Interceptação de Comunicação** - Muitos dispositivos IoT facilitam a comunicação entre pessoas. Como exemplos mais populares, temos as câmeras de campainha sem fio e alto-falantes inteligentes. No entanto, se um dispositivo for vulnerável, há uma grande probabilidade de um hacker atacá-lo para acessar conversas pessoais das pessoas.

- **Captura de Node -**. Esse tipo de ataque tem como objetivo roubar os dados armazenados em dispositivos IoT. Para alcançar esse objetivo, os atacantes obtêm acesso a um nó crucial que facilita o acesso à memória do dispositivo.

- **Ataque de Tempo** - Trata-se de um tipo de ataque complexo que exige que os atacantes analisem o tempo que os dispositivos IoT levam para responder. Se os dispositivos possuem baixo poder de computação e demoram muito para responder, os hackers podem encontrar vulnerabilidades para explorar.

Camada de Rede

Subindo um pouco mais na arquitetura em camadas, chegamos na camada de rede. Esta camada é uma das mais importantes na arquitetura da IoT pois conecta usuários com dispositivo. Neste ponto, muitos dos ataques estão relacionados aos ataques de hackers, em ações parecidas de como acontece na internet. Eles se empenham em obter acesso não autorizado a sistemas IoT e manipulá-los sem permissão. A seguir, são apresentados os três tipos mais comuns de ataques.

- **Ataque de Interceptação (Man-in-The-Middle - MiTM)** - Este é um ataque grave à arquitetura de referência IoT, pois permite que hackers manipulem dispositivos em tempo real. Durante esse tipo de ataque, um hacker intercepta solicitações entre um remetente e um receptor e as altera.
- **Ataque ao Armazenamento -** A maioria dos sistemas IoT armazena os dados coletados pelos sensores dos dispositivos. Esses dados são armazenados em discos rígidos nos dispositivos ou na nuvem. Hackers frequentemente atacam o armazenamento para baixar os dados coletados.
- **Ataque por Exploração** - É um tipo de ataque que exige que golpistas analisem modelos específicos de comunicação IoT. Após fazer isso, eles encontram brechas e as utilizam para acessar os sistemas IoT sem autorização.

Camada de Suporte

Seguindo a estrutura de 4 camadas que estudamos no início do curso, entramos na camada de suporte. Esta camada contribui substancialmente para aprimorar a segurança. Contudo, ela não protege todas as camadas da

arquitetura IoT contra todas as ameaças existentes. As duas ameaças mais comuns são nesta camada são

- **Ataque de Negação de Serviço (DoS) -** Resumidamente, esse ataque requer que um hacker envie um grande número de solicitações à camada de rede, de modo que ela não consiga processar todas ao mesmo tempo. Nesse caso, um sistema sobrecarregado parará de funcionar.
- **Ataque Interno** - Para realizá-lo, um golpista precisa obter as credenciais de login de um usuário existente do sistema IoT. Após isso, eles podem carregar um código malicioso no sistema para danificá-lo ou obter informações sensíveis.

Camada de Aplicação

Essa camada apresenta diversas questões que precisam ser resolvidas, sendo as preocupações com segurança as mais importantes. Existem muitas maneiras diferentes de atacar dispositivos nesta camada para obter acesso não autorizado. As mais comuns incluem:

- **Scripting entre Sites (Cross-site scripting)** - A maioria dos sites que facilitam a interação com dispositivos IoT é segura. No entanto, alguns apresentam falhas que os hackers exploram. Para acessar dados sensíveis dos usuários ou obter controle sobre dispositivos IoT, eles inserem um código e o executam como se fossem administradores do site.
- **Ataque de Código Malicioso -** Todas as aplicações estão vulneráveis a ataques de códigos maliciosos. Portanto, vírus de computador que se espalham pela Internet podem facilmente danificar dispositivos IoT específicos ou até mesmo destruir um modelo IoT complexo.

Além desses ataques, também são comuns

- **Malware** - Devido a coleta de uma grande quantidade de dados, existe a chance de trojans ou vírus de computador infiltrarem-se no sistema.

Além disso, eles podem fornecer acesso não autorizado a *data lakes* e bancos de dados para os golpistas.

- **Exaustão** - Outro ataque, semelhante ao de Negação de Serviço (DoS), pode causá-lo. Este tipo de ataque visa esgotar a bateria de um dispositivo ou consumir 100% da capacidade de processamento e memória de um computador, de modo que ele não será capaz de executar outras tarefas.

1.3 Recomendações

Implementar segurança em uma solução IoT (Internet das Coisas) é fundamental para proteger os dispositivos contra ataques e garantir a segurança dos dados. Na Tabela 6 .1 resume as práticas recomendadas para implementar segurança em uma solução IoT, abordando desde a autenticação e comunicação até o design seguro e a conscientização sobre segurança.

Tabela 6.1 - Resumo das práticas de implementação de segurança em Soluções IoT

Categoria	Medida	Descrição
Autenticação e Autorização	Autenticação Forte	Utilizar autenticação de dois fatores, certificados digitais e gestão eficaz de identidade e acesso para garantir acesso autorizado.
Comunicação	Comunicação Segura	Criptografar comunicação usando protocolos seguros como TLS para proteger dados em trânsito.
Manutenção de Segurança	Atualizações e Patches	Manter dispositivos e software atualizados com os últimos patches de segurança para corrigir vulnerabilidades.
Proteção de Dados	Criptografia e Controle de Acesso	Implementar criptografia de dados em repouso e controles de acesso baseados em políticas para proteger dados sensíveis.
Isolamento de Rede	VPNs e Firewalls	Usar VPNs e firewalls para isolar dispositivos IoT da rede corporativa, limitando a exposição a ataques.
Detecção e Resposta	Sistema de Detecção de Intrusão	Utilizar sistemas de monitoramento de segurança para identificar e responder a atividades suspeitas.
Análise de Riscos	Avaliações e Testes de Vulnerabilidade	Realizar testes de vulnerabilidade e avaliações de risco regularmente para identificar e mitigar vulnerabilidades.

Conscientização em Segurança	Treinamento	Educar usuários e desenvolvedores sobre práticas de segurança, incluindo reconhecimento de phishing e importância de senhas fortes.
Design Seguro	Segurança desde o Design	Incorporar considerações de segurança nas fases iniciais do desenvolvimento, minimizando dados coletados e projetando dispositivos para serem seguros.

1.4 Privacidade de Dados em IoT

A privacidade de dados no contexto da Internet das Coisas (IoT) refere-se à proteção de informações pessoais coletadas, processadas e armazenadas por dispositivos conectados e sistemas IoT. Com o crescimento na utilização e difusão das soluções de IoT, uma vasta quantidade de dados é gerada continuamente por dispositivos inteligentes, sensores e outros elementos conectados à internet. Esses dados podem incluir informações altamente pessoais e sensíveis, como hábitos de consumo, padrões de comportamento, dados de saúde, localização geográfica, entre outros.

Entre alguns pontos importantes que devem ser levados em consideração quando estamos analisando a privacidade dos dados, podemos destacar: (a) o **consentimento informativo**, que garante que os usuários estejam plenamente cientes de quais dados estão sendo coletados, como estão sendo usados e com quem estão sendo compartilhados; (b) a implementação de medidas de **segurança robustas** para proteger os dados contra acessos não autorizados, vazamentos ou outros tipos de ataques cibernéticos; (c) a **coleta apenas dos dados estritamente necessários** para o propósito específico pretendido, evitando a coleta excessiva de informações pessoais; (d) a **transparência e responsabilidade**, estabelecendo responsabilidades claras para a gestão desses dados; (e) o respeito ao direito dos indivíduos de **acessar, corrigir e até mesmo apagar** seus dados pessoais dos sistemas quando solicitado; e (f) a **garantia** que os dados coletados não sejam utilizados para fins prejudiciais ou discriminatórios.

Uma forma de garantir essa privacidade é utiliza-la como controle. Nesta abordagem, se usa da capacidade de controlar o que acontece com os dados pessoas para evitar a utilização indevida por terceiros. Para isso é necessário

utilizar tecnologias para a especificação e aplicação de políticas de privacidades. Uma forma de nortear esse controle é apresentada por Santos e Sales (2015), citando o trabalho de Wang e Kobsa (2008), que identificam 11 aspectos fundamentais da privacidade (Tabela 6.2).

Tabela 6.2 - Onze princípios fundamentais da privacidade (Fonte: Santos e Sales (2015))

Princípio	Descrição
Consciência de Utilização	Baseada em declarações claras e bem detalhadas das políticas de privacidade.
Minimização dos Dados	Busca avaliar a necessidade, eficácia e proporcionalidade de novas tecnologias antes de sua implantação, dando preferência a soluções menos invasivas.
Especificação de Objetivos	Observa a finalidade para qual os dados estão sendo coletados.
Limitação de Coleta	Objetiva definir os limites para a coleta de dados a ser realizada.
Limitação de Uso	Defini-se a fim de evitar que dados sejam usados ou divulgados para fins que não tenham sido especificados no momento da coleta.
Proteção de Transferência	Deve ser definida para evitar que dados sejam transferidos caso a garantia de proteção adequada não possa ser mantida.
Capacidade de Escolha e Consentimento	Baseia-se no princípio de que os indivíduos devem possuir a capacidade de decidir sobre a coleta, uso e divulgação de seus dados.
Acesso	Garante que as pessoas podem verificar seus dados armazenados.
Integridade	Princípio base para garantir que os dados recolhidos serão destinados para a finalidade a que se destinam.
Segurança	Garantia de que os dados estão fora de risco de perda, acesso não autorizado, uso indevido, modificação ou divulgação não autorizada.
Aplicação	Preocupa-se diretamente com a existência de mecanismos que façam cumprir princípios de privacidade.

Referências

A. G. D. S. Junior, L. M. G. Gonçalves, G. A. De Paula Caurin, G. T. B. Tamanaka, A. C. Hernandes and R. V. Aroca, "**BIPES: Block Based Integrated Platform for Embedded Systems**," in IEEE Access, vol. 8, pp. 197955-197968, 2020, doi: 10.1109/ACCESS.2020.3035083.
Full text: https://ieeexplore.ieee.org/document/9246562

SANTOS, Bruno P.; SILVA, Luiz A. M.; CELES, Carla S. F. S.; BORGES NETO, João B.; PERES, Bruno S.; VIEIRA, Marcelo A. M.; VIEIRA, Luiz F. M.; GOUSSEVSKAIA, Olga N.; LOUREIRO, Antônio A. F. (2016). **Internet das Coisas: da Teoria à Prática**. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS [SBRC], 31., 30 de maio de 2016, Salvador. Anais [...]. Salvador: UFMG, 2016. p. 1-50.

ASHTON, Kevin. **Entrevista exclusiva com o criador do termo "Internet das Coisas"**. Finep, 2015. Disponível em: <http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevista-exclusiva-com-o-criador-do-termo-internet-das-coisas>. Acesso em: 26 de outubro de 2023.

TOTVS. **Aplicações da Internet das Coisas**. Blog Totvs, 2023. Disponível em: <https://www.totvs.com/blog/inovacoes/aplicacoes-da-internet-das-coisas/>. Acesso em: 8 de novembro de 2023.

Usemobile. **IoT: 9 exemplos de aplicativos bem-sucedidos**. Usemobile, 2023. Disponível em: <https://usemobile.com.br/iot-9-exemplos-de-aplicativos/>. Acesso em: 8 de novembro de 2023.

Google. **Breaking down language barriers with augmented reality**. YouTube, 2023. Disponível em: <https://www.youtube.com/watch?v=lj0bFX9HXeE>. Acesso em: 8 de novembro de 2023.

ZUP. **A arquitetura da Internet das Coisas**. 30 de agosto de 2023. Disponível em: https://www.zup.com.br/blog/a-arquitetura-da-internet-das-coisas. Acesso em: 28 de novembro de 2023.

AMAZON WEB SERVICES. **O que é MQTT?** 20 de julho de 2023. Disponível em: https://aws.amazon.com/pt/what-is/mqtt/. Acesso em: 28 de novembro de 2023.

GTA/UFRJ. **COAP: Protocolo de comunicação para a Internet das Coisas**. 8 de março de 2019. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/coap/. Acesso em: 28 de novembro de 2023.

HIVEMQ. **MQTT vs HTTP: Protocolos para IoT e IIoT**. 21 de junho de 2023. Disponível em: https://www.hivemq.com/article/mqtt-vs-http-protocols-in-iot-iiot/. Acesso em: 28 de novembro de 2023.

EMBARCADOS. **AMQP: Protocolo de comunicação para IoT**. 10 de maio de 2023. Disponível em: https://embarcados.com.br/amqp-protocolo-de-comunicacao-para-iot/. Acesso em: 28 de novembro de 2023.

CONCEIÇÃO JÚNIOR, André Lisboa da. **Redes sem Fio: Protocolo Bluetooth Aplicado em Interconexão entre Dispositivos**. Disponível em: https://www.teleco.com.br/tutoriais/tutorialredespbaid/pagina_5.asp. Acesso em: 8 jan. 2024.

EMBARCADOS. **Protocolos de Rede sem Fio de IoT**. Disponível em: https://embarcados.com.br/protocolos-de-rede-sem-fio-de-iot/ Acesso em: 8 jan. 2024.

ARAÚJO, André Silva de; VASCONSELLOS, Pedro de. **Conclusão - Bluetooth Low Energy (BLE)**. Disponível em:

https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/bluetooth/conclusao.htm. Acesso em: 8 jan. 2024.

ELEMENT14 COMMUNITY. **Tech Spotlight: SigFox - A Wide Area Network Protocol for IoT.** Disponível em: https://community.element14.com/learn/learning-center/the-tech-connection/w/documents/3897/tech-spotlight-sigfox----a-wide-area-network-protocol-for-iot. Acesso em: 8 jan. 2024.

EMBARCADOS. **Uma Visão Técnica da Rede Sigfox**. Disponível em: https://embarcados.com.br/uma-visao-tecnica-da-rede-sigfox/. Acesso em: 8 jan. 2024.

GTA UFRJ. **Protocolos de Rede para Redes de Sensores Sem Fio**. Disponível em: https://www.gta.ufrj.br/grad/10_1/rssf/protocolos.html. Acesso em: 8 jan. 2024.

EMBARCADOS. **NFC (Near Field Communication) – Aplicações e uso**. Disponível em: https://embarcados.com.br/nfc-near-field-communication/ Acesso em: 23 jan. 2024.

GTA UFRN. **Protocolo Zigbee.** Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2017_2/802154/zigbee.html. Acesso em: 24 jan. 2024.

Microsoft Azure. **O que é IoT? Segurança.** https://azure.microsoft.com/en-us/solutions/iot. Acessado em 21 de fevereiro de 2024.

SANTOS, Carlos Cesar; SALES, Jefferson David de Araújo. O desafio da privacidade na internet das coisas. GESTÃO.Org : Revista Eletrônica de Gestão Organizacional, v. 13, n. Especial, p. 282-290, dez. 2015.

Johnson, A. (2021, Janeiro 1). Understanding IoT Architecture Layers. Jelvix. https://jelvix.com/blog/iot-architecture-layers

BOM CURSO!

Instituto de Tecnologia