

Segurança em Internet das Coisas: Uma Revisão da Literatura

Victor T. Hayashi¹, Felipe V. de Almeida¹, Andrea E. Komo¹

¹ Escola Politécnica – Universidade de São Paulo (USP)

{victor.hayashi, felipe.valencia.almeida, andrea.komo}@usp.br

Abstract. *Internet of Things (IoT) security is still an open research problem. The heterogeneity of devices, languages and protocols creates a large attack surface, and the processing, memory and bandwidth limitations of embedded devices limit the use of traditional security mechanisms. In this paper, a review of the literature on IoT security is presented, highlighting vulnerabilities and attacks that motivate research, the contributions of Brazilian research, and identification of research gaps to foster an agenda for future work.*

Resumo. *A segurança em Internet das Coisas (IoT) ainda é um problema de pesquisa em aberto. A heterogeneidade de dispositivos, linguagens e protocolos cria uma grande superfície de ataque, e as limitações de processamento, memória e banda dos dispositivos embarcados limitam o uso de mecanismos tradicionais de segurança. Neste artigo, é apresentada uma revisão da literatura sobre a segurança em IoT, destacando vulnerabilidades e ataques que motivam as pesquisas, as contribuições da pesquisa brasileira, e identificação de lacunas de pesquisa para fomentar uma agenda de trabalhos futuros.*

1. Introdução e Motivação

A Internet das Coisas (IoT, do inglês *Internet of Things*) apresenta oportunidades de ganhos em eficiência operacional, redução de custos e otimização de fluxos operacionais em diversos setores como a Indústria 4.0, cidades inteligentes e residências conectadas. Segundo Gartner ¹, são estimados 6,2 bilhões de dispositivos conectados em 2021, número que tende a continuar crescendo nos próximos anos.

Garantir a segurança destes sistemas e dispositivos não é algo trivial devido à heterogeneidade de linguagens, protocolos, *frameworks* e plataformas, que levam a uma crescente superfície de ataque. A preocupação com a segurança em IoT levou à criação de uma lei norte-americana para garantir padrões mínimos de segurança para os dispositivos IoT ². No Brasil, o Plano Nacional de Internet das Coisas foi instituído pelo decreto de número 9.854 em 2019 ³, e uma frente horizontal considerada em estudo relacionado é de Regulatório, Segurança e Privacidade de Dados ⁴.

¹<https://www.gartner.com/en/newsroom/press-releases/2021-04-01-gartner-forecasts-global-devices-installed-base-to-reach-6-2-billion-units-in-2021>

²<https://www.congress.gov/bill/116th-congress/house-bill/1668/text>

³<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/ArquivosInternetDasCoisas/d9854.pdf>

⁴<https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo>

Há desafios relacionados aos dispositivos restritos utilizados em IoT, que possuem limitações de recursos como energia, memória, processamento e dimensões físicas [Gerža et al. 2014]. Devido ao uso destes dispositivos restritos e requisitos específicos de IoT relacionados a requisitos de tempo real, escalabilidade e usabilidade, é um grande desafio utilizar os mecanismos tradicionais de criptografia neste novo contexto [Babaei and Schiele 2019].

Por outro lado, como sistemas de IoT possuem atuadores e podem estar implantados em sistemas críticos como indústrias, os impactos de ataques podem não se limitar à integridade ou confidencialidade dos dados, mas também a atuações indevidas que causam indisponibilidades em processos de negócio, redução de vida útil de equipamentos e até danos físicos a operadores. Considerando um contexto residencial, é possível que os ataques tenham impactos não somente na privacidade dos residentes, mas também na sua vida cotidiana, como a indisponibilidade de controle de fornos e aparelhos de ar condicionado conectados. Desta forma, é necessário se atentar que muitos ataques envolvendo segurança da informação (*security*) de sistemas IoT podem ter impactos relevantes na segurança física (*safety*) de pessoas [Heartfield et al. 2018].

Este artigo é organizado da seguinte forma: a seção 2 apresenta algumas vulnerabilidades e ataques encontrados na literatura e identificados pela comunidade internacional *Open Web Application Security Project* (OWASP), e que motivam as pesquisas na área de segurança em IoT. A seção 3 descreve os resultados das contribuições brasileiras na área, e detalha as lacunas de pesquisa identificadas. Por fim, a seção 4 conclui o artigo destacando as principais contribuições brasileiras identificadas, além de uma agenda de pesquisas futuras a partir de lacunas identificadas.

2. Vulnerabilidades e Ataques

Um exemplo que ganhou destaque global nesse quesito foi o ataque cibernético nomeado de *Mirai* [Tushir et al. 2021]. Esse ataque consistiu na invasão de diversos dispositivos IoT conectados na Internet como câmeras IP, impressoras, entre outros, principalmente os que mantinham as configurações padrão de fábrica dos aparelhos ou usavam senhas de acesso muito comuns, óbvias e inseguras. Depois desses dispositivos serem comprometidos, eles foram usados para compor uma grande *botnet* e causar um grande ataque de DDoS mundial. Se nesse episódio do *Mirai* os dispositivos estivessem com credenciais seguras, diferentes dos padrões amplamente conhecidos [Mordeno and Russell 2015], todo o problema poderia ter sido evitado.

A fundação OWASP publicou uma lista de 10 elementos a se evitar em relação à segurança em IoT. Esta lista está inclusa no projeto OWASP IoT iniciado em 2014 para auxiliar desenvolvedores, fabricantes, empresas e consumidores a fazer melhores decisões em relação à criação e uso de sistemas IoT. As seguintes vulnerabilidades estão presentes na lista de 2018 ⁵: inexistência de gerenciamento de credenciais e sua proteção, serviços de rede inseguros, interfaces inseguras, falta de mecanismo de atualização seguro, uso de componentes desatualizados, proteção insuficiente de privacidade, transferência e armazenamento de dados de forma insegura, falta de gerenciamento de dispositivos, configurações padrão de fábrica inseguras, e falta de proteção física.

⁵<https://owasp.org/www-project-internet-of-things/>

Uma forma de organizar os possíveis ataques, vulnerabilidades e ameaças em IoT é proposta na literatura [Hassija et al. 2019] a partir de uma arquitetura de cinco camadas: sensoriamento, rede, *middleware*, *gateway* e aplicação. A seguir, são apresentadas estas camadas e alguns exemplos de insegurança:

- **Sensoriamento:** ataques de canal lateral como a obtenção de chaves criptográficas a partir de análise de consumo de energia de um dispositivo IoT; interferência por sinais de radiofrequência que causam indisponibilidade do sistema ao usuário legítimo; exploração de vulnerabilidades durante o reinício de dispositivos IoT para obter seu controle em um ataque de captura de nó;
- **Rede:** ataque de *phishing*, por exemplo em uma interface *web* onde usuários podem monitorar e controlar seus dispositivos IoT para obter as credenciais de acesso ao portal verdadeiro; ataque de negação de serviço (DoS) como muitas requisições a um componente de rede específico; ataques de roteamento que causam indisponibilidade para o usuário legítimo, ou até comprometimento da integridade dos dados por meio da alteração destes por um atacante;
- **Middleware:** ataque de *flooding* na nuvem que causa indisponibilidade da plataforma IoT integrada aos dispositivos; uso de *malware* na nuvem para disponibilização de dados coletados a terceiros não autorizados; personificação da plataforma IoT em nuvem, de forma que os dispositivos IoT podem enviar dados em tempo real a um terceiro não autorizado;
- **Gateway:** atualizações de *firmware* de forma insegura podem resultar no controle total dos dispositivos por atacantes; se o processo de configuração inicial for inseguro, as credenciais podem ser obtidas por atacantes durante este processo; se a criptografia não for realizada de ponta a ponta, é possível que dados em trânsito sejam capturados por atacantes;
- **Aplicação:** ataques ao controle de acesso como a elevação de privilégio ou resultantes de políticas de controle de acesso não granulares o suficiente; ataques de interrupção de serviço que podem afetar todos os usuários de um sistema IoT em nuvem; ataques de negação de serviço realizados de forma distribuída (DDoS), como o uso de uma rede de dispositivos comprometidos para atacar um servidor centralizado de forma massiva.

Pelo exposto em relação às vulnerabilidades e ataques possíveis descritos na literatura, fica fundamentada a necessidade de sistematizar pesquisas nacionais na área de segurança em IoT, como já ocorre no cenário internacional [Hassan et al. 2019].

3. Pesquisas do SBSeg

Conforme pode ser observado na Tabela 1, os 12 artigos apresentados em edições da conferência nacional sobre Segurança da Informação (SBSeg) com o tema de segurança em IoT podem ser classificados nas categorias Detecção de Intrusão (4 trabalhos), Controle de Acesso (3 trabalhos), Autenticação (3 trabalhos), e Privacidade (2 trabalhos).

As oportunidades de pesquisa futuras estão relacionadas às vulnerabilidades e ataques descritos na seção 2, além dos trabalhos futuros detalhados na Tabela 1. É possível que as pesquisas futuras se atentem à miríade de ataques e vulnerabilidades identificados, ou que possam dar continuidade às pesquisas brasileiras apresentadas. Grande parte dos trabalhos futuros destaca a necessidade de se avaliar aspectos de energia e desempenho para provar a viabilidade das abordagens propostas.

Ano	Tema	Contribuição	Trabalhos Futuros	Ref.
2018	Controle de Acesso	Solução baseada em ABAC, padrões SAML e FIDO UAF, comunicação RFID e NFC	Uso do sistema proposto de controle de acesso em cenário acadêmico	[da Silva et al. 2018]
2018	Autenticação	Arquitetura para IoT móvel com chaves públicas para cidades inteligentes	Avaliar atrasos nas mensagens do padrão DDS (publish-subscriber)	[Leopoldino and da Rocha 2019]
2018	Controle de Acesso	Permitir o controle de fluxos de dados em aplicações IoT de maneira granular	Avaliar o esforço de portar aplicações IoT e impactos no desempenho	[Mauro Junior et al. 2018]
2018	Detecção de Intrusão	Dataset público para fomentar pesquisas de detecção de intrusão, com foco em botnets	Incluir mais tipos de botnets e dispositivos IoT	[Bezerra et al. 2018b]
2018	Detecção de Intrusão	Uso de modelo one class SVM para detecção de botnets com testes em dispositivos reais	Avaliar a abordagem em diferentes dispositivos e botnets, explorar outros parâmetros para detecção	[Bezerra et al. 2018a]
2018	Privacidade	Solução de pseudo-anonimização baseada em SDN, validado com tráfego real, e com pouco impacto no desempenho da comunicação	N/A	[Pinheiro et al. 2018]
2019	Controle de Acesso	Uso de confiança social entre dispositivos IoT para torná-los resilientes a ataques Sybil	Associar técnicas de hardware, aplicar lógica fuzzy e validar em outros cenários	[de Oliveira et al. 2019]
2019	Detecção de Intrusão	Detecção de intrusão para lidar com a ameaça de injeção de dados falsos no contexto industrial	Avaliar a abordagem em outros cenários de redes IoT densas, avaliar consumo de energia e mobilidade	[Pedroso et al. 2019]
2019	Detecção de Intrusão	Identificação de comportamento anômalo de dispositivos usando SDN para bloqueio de ataques	Avaliar a eficiência de criação de políticas de bloqueio no caso de ataques DoS, uso de ML para autonomia da solução	[Gonçalves et al. 2019]
2019	Privacidade	Utiliza dois módulos, teste de vulnerabilidade e de proteção de privacidade para proteger informações de comportamento de dispositivos IoT	Avaliar o impacto da solução proposta em atributos de rede como largura de banda e latência.	[Prates Jr et al. 2019]
2019	Autenticação	Autenticação mútua entre publicadores e broker MQTT com renovação periódica de chaves com menos energia e pouco impacto no tempo de resposta	Avaliação do desempenho em dispositivos IoT restritos, estabelecer valores de renovação de chaves frente a outros ataques DoS, como o SYN Flood	[Junior et al. 2019]
2019	Autenticação	Abordagens para aceleração de assinaturas baseadas em atributos para dispositivos restritos IoT	Necessidade de projeto de hardware dedicado para aceleração, como FPGA	[Neto et al. 2019]

Tabela 1. Resumo de contribuições e trabalhos futuros de artigos de conferência brasileira sobre Segurança da Informação.

4. Considerações Finais

Este artigo apresentou uma meta análise de 12 artigos sobre segurança em IoT oriundos de conferências nacionais para identificar as principais contribuições e lacunas de pesquisa. Adicionalmente, vulnerabilidades e ataques descritos na literatura foram apresentados para motivar mais pesquisas na área.

Ao considerar IoT como um sistema distribuído com restrições específicas (e.g., dimensões, energia, capacidade de processamento, memória disponível) e com requisitos de tempo de resposta e disponibilidade a depender da aplicação, observa-se que as pesquisas em geral carecem de provas de conceito que considerem o equilíbrio da segurança com outros requisitos não-funcionais para estudar sua viabilidade no cenário IoT.

Como trabalhos futuros, trabalhos de outros eventos nacionais como o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) podem complementar o presente levantamento. É esperado que o presente artigo auxilie na proposição de uma agenda de pesquisa brasileira, para garantir que as iniciativas nacionais de investimentos e projetos em IoT possam levar em consideração o aspecto de segurança, que é essencial para o sucesso da adoção desta nova tecnologia.

Referências

- [Babaei and Schiele 2019] Babaei, A. and Schiele, G. (2019). Physical unclonable functions in the internet of things: State of the art and open challenges. *Sensors (Switzerland)*, 19(14).
- [Bezerra et al. 2018a] Bezerra, V. H., da Costa, V. G. T., Junior, S. B., Miani, R. S., and Zarpelao, B. B. (2018a). One-class classification to detect botnets in iot devices. In *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 43–56. SBC.
- [Bezerra et al. 2018b] Bezerra, V. H., da Costa, V. G. T., Martins, R. A., Junior, S. B., Miani, R. S., and Zarpelao, B. B. (2018b). Providing iot host-based datasets for intrusion detection research. In *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 15–28. SBC.
- [da Silva et al. 2018] da Silva, G. C., da Silva, C. E., de Mello, E. R., Wangham, M. S., and Loli, S. B. (2018). Transposição da autenticação federada para uma solução de controle de acesso físico no contexto da internet das coisas. In *Anais Estendidos do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 73–80. SBC.
- [de Oliveira et al. 2019] de Oliveira, G., Nogueira, M., and Santos, A. (2019). Controle de acesso à iot baseado na percepção de comunidade e confiança social contra ataques sybil. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 71–84. SBC.
- [Gerža et al. 2014] Gerža, M., Schauer, F., and Jašek, R. (2014). Security of ises measure-server® module for remote experiments against malign attacks. *International Journal of Online Engineering*.
- [Gonçalves et al. 2019] Gonçalves, D., Kfourri, G., Dutra, B., de Alencastro, J., de Caldas Filho, F., Martins, L., Albuquerque, R., and de Sousa Jr, R. (2019). Arquitetura

de ips para redes iot sobrepostas em sdn. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 309–322. SBC.

- [Hassan et al. 2019] Hassan, W. H. et al. (2019). Current research on internet of things (iot) security: A survey. *Computer networks*, 148:283–294.
- [Hassija et al. 2019] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743.
- [Heartfield et al. 2018] Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., and Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home.
- [Junior et al. 2019] Junior, C. R., Quincozes, S., and Kazienko, J. (2019). Legitimatebroker: Mitigando ataques de personificação em broker mqtt na internet das coisas. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 141–154. SBC.
- [Leopoldino and da Rocha 2019] Leopoldino, G. and da Rocha, R. (2019). Uma arquitetura para comunicação espontânea e segura para internet das coisas móveis em cidades inteligentes. In *Anais Estendidos do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 135–144. SBC.
- [Mauro Junior et al. 2018] Mauro Junior, D., Gama, K., and Prakash, A. (2018). Securing iot apps with fine-grained control of information flows. In *XVIII Brazilian Symposium On Information and Computational Systems Security*.
- [Mordeno and Russell 2015] Mordeno, A. and Russell, B. (2015). Identity and access management for the internet of things-summary guidance. *Cloud Security Alliance (CSA)*.
- [Neto et al. 2019] Neto, A. M., Richardson, S., Horowitz, M., and Oliveira, L. (2019). Aceleração de assinaturas baseadas em atributos para internet das coisas. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 427–432. SBC.
- [Pedroso et al. 2019] Pedroso, C., Gielow, F., Santos, A., and Nogueira, M. (2019). Mitigação de ataques idfs no serviço de agrupamento de disseminação de dados em redes iot densas. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 211–224. SBC.
- [Pinheiro et al. 2018] Pinheiro, A. J., Burgardt, C. A., and Campelo, D. R. (2018). Preservando a privacidade na internet das coisas com pseudônimos usando sdn. In *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 121–128. SBC.
- [Prates Jr et al. 2019] Prates Jr, N., Vergütz, A., Macedo, R., and Nogueira, M. (2019). Um mecanismo de defesa contra ataques traffic side-channel temporais na iot. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 323–336. SBC.
- [Tushir et al. 2021] Tushir, B., Sehgal, H., Nair, R., Dezfouli, B., and Liu, Y. (2021). The impact of dos attacks on resource-constrained iot devices: A study on the mirai attack. *CoRR*, abs/2104.09041.