Ambiente para Experimentação em Ataques na IoT

RESUMO EXPANDIDO - Disciplina de TCC290009

Allex Magno Andrade
Estudante do Curso de Engenharia de Telecomunicações

Emerson Ribeiro de Mello
Michelle Silva Wangham

Semestre 2020-1

Resumo- *O período atual da Internet, em que há um número elevado de dispositivos conectados a rede, oferece aos usuários recursos cada vez mais automatizados, com poucas interferências e cada vez mais acessível. Por outro lado, esses objetos com alguma capacidade computacional podem trazer riscos inerente a sua operação, expondo dados sensíveis de usuários e empresas, ou ainda, potencializando ataques de negação de serviços. Dessa forma, pesquisas são realizadas para desenvolver recursos que trazem maior credibilidade e procuram minimizar as falhas de segurança presentes nesse ecossistemas. Porém, os experimentos são onerosos e demandam tempo e recursos, o que normalmente são escassos. Além disso, não é fácil alcançar o nível de confiança desejável. Com o objetivo de diminuir todos esses problemas, ambientes para experimentação são construídos com financiamentos de diversas organizações, como é o exemplo do DETERLab, um testbed preparado para experimentos em cyber segurança e que pode ser adaptado para emular dispositivos IoT. Já o Brasil carece desses ambientes voltados para segurança, exigindo que pesquisadores procurem testbeds disponibilizados por outros países. Contudo, o FIBRE é um testbed que foi desenvolvido para realizar experimentos em redes de computadores, e possui uma infraestrutura que pode ser adaptada para realizar experimentos de segurança em IoT. O objetivo deste trabalho é estudar as tecnologias que conferem a confiabilidade do DETERLab e adaptá-las ao FIBRE para que seja capaz de suportar experimentos com diferentes tipos de ataques sem oferecer riscos ao ambiente e a rede externa. Esse ambiente poderá ser utilizado pela comunidade acadêmica para ensino e pesquisa em cyber segurança, além de permitir explorar novas arquiteturas e serviços voltadas para a IoT.*

Palavras-chave: Internet das Coisas. *Testbed.* Segurança Computacional.

1 Introdução

A Internet das Coisas é composta por uma rede universal e heterogênea, com tecnologias interoperáveis, capazes de conectar objetos inteligentes (ITU, 2012). Sua arquitetura pode ser dividida em três camadas bem definidas, embora alguns autores adicionam subcamadas intermediárias para tratar de pontos específicos. Os objetos são definidos por meio de algumas características básicas que determinam sua estrutura e seu comportamento.

Com o crescente avanço da tecnologia, em 2020, o número de unidades pode chegar a 26 bilhões, o que representa impactos tanto nas indústrias, que fabricam peças e componentes, quanto no mercado, que utiliza desses dispositivos para gerar produtos e serviços (Meneghello et al., 2019). Além disso, outros fatores devem ser levados em conta, pois com esse número elevado de componentes coletando informações de pessoas, máquinas e ambientes, as oportunidades de violar a segurança e obter dados sensíveis crescem exponencialmente a medida que os dispositivos são conectados a rede.

Em um ecossistema aberto, diferentes cenários motivam diversos atores, implicando em desafios de segurança cada vez maiores. A IoT (*Internet of Things*) impõe desafios extras para segurança devido suas características. Muitos dos dispositivos possuem poucos mecanismos que evitam ataques de negação de serviço ou vazamentos de informações. Um dos grandes problemas potencializados por esses equipamentos são os ataques por meios das *botnets*, como ocorreu em outubro de 2016. Por isso, não apenas usuários, mas também dispositivos devem ser autenticados e autorizados a acessar informações de maneira segura. Babar et al. (2011) apontam que a gestão de identidades, a comunicação segura, o acesso seguro à rede e resistência à violação devem ser garantidos.

Pesquisas em segurança buscam minimizar as vulnerabilidades dos sistemas, utilizando diferentes meios confiáveis. Para isso, existem simulações que permitem que sejam feitas avaliações de tecnologias com resultados semelhantes aos que são encontrados em um sistema real, sem gerar custos elevados, porém, podem oferecer níveis de confiabilidade questionável, uma vez que suas configurações devem estar alinhada ao que se deseja simular. Por outro lado, as pesquisas experimentais, baseiam-se em ambientes para experimentação, *testbeds*. Esses ambientes são alternativas às simulações com melhores perspectivas de análise, além de permitir experimentos com sistemas e usuários reais, em um ambiente controlado e em larga escala (RAKOTOARIVELO et al., 2010).

Os *testbeds* foram criados, a partir de financiamentos de diferentes entidades governamentais e não governamentais, para atender diferentes demandas, seja em busca de resposta rápida a algum problema ou para fins educacionais, como é o exemplo do *Global Environment for Network Innovations* (GENI), *OneLab*, *cyber DEfense Technology Experimental Research* (DETERLab) e o *Future Internet Brazilian Environment for Experimentation* (FIBRE) no Brasil.

O DETERLab é um ambiente para pesquisas experimentais em *cyber* segurança, cujos objetivos é disponibilizar uma plataforma sofisticada e simples de ser configurada. Segue critérios rigorosos de segurança, que provê isolamento para que nenhum experimento seja afetado por outros, e também para que não "vazem"para a internet. Além de fornecer diversos outros benefícios, principalmente na área acadêmica, permitindo que

seus experimentos sejam repetíveis, quantas vezes forem necessários, sem alteração do resultado (WROCLAWSKI et al., 2016). Já o FIBRE é um ambiente para experimentação, resultado de uma parceria entre Brasil e Europa, cujo objetivo principal é fornecer aos pesquisadores um *testbed* onde são realizado experimentos de novas aplicações e modelos de arquitetura de rede para a Internet do Futuro (FIBRE, 2020).

Nesse sentido, em vista da falta de um ambiente no Brasil, que oferece suporte para experimentação de segurança em IoT, de larga escala e de fácil acesso aos pesquisadores, o objetivo desse trabalho é propor uma adequação ao *testbed* FIBRE para que suporte ataques experimentais, utilizando o DETERLab como referência.

2 Metodologia

A metodologia para desenvolver este trabalho está dividida em duas partes. A primeira consiste em estudar e analisar como é a arquitetura do DETERLab, observando os mecanismos de segurança para executar os experimentos e como estes são administrados. A segunda estuda as características do FIBRE e propõe os ajustes necessários para viabilizar experimentos que realizam ataques em seu ambiente.

2.1 DETERLab

Os estudos sobre o DETERLab serão feitos com base nos documentos disponíveis em seu portal, artigos publicados e com experimentos realizados no ambiente.

2.2 FIBRE

Para realizar os estudos referentes ao FIBRE será utilizado os documentos disponíveis no portal, publicações, experimentos executados no ambiente e contato com os administradores da plataforma.

3 Considerações Parciais/Finais

Ao final, com a realização dos ajustes necessários, espera-se obter um ambiente confiável para executar experimentos de segurança na IoT. Esse ambiente será disponibilizado em todo território nacional para ensino e pesquisa, que permitirá explorar novas arquiteturas e aplicações de segurança em sistemas distribuídos.

Referências

BABAR, S. et al. Proposed embedded security framework for internet of things (iot). In: IEEE. *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*. [S.l.], 2011. p. 1–5.

FIBRE. *What is FIBRE*. 2020. Https://www.fibre.org.br/about/what-is-fibre/. Acesso em: 29 abr 2020.

ITU. Overview of the internet of things. 2012. Disponível em: <http://handle.itu.int/11.1002/1000/11559>.

Meneghello, F. et al. Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, v. 6, n. 5, p. 8182–8201, 2019.

RAKOTOARIVELO, T. et al. Omf: A control and management framework for networking testbeds. *SIGOPS Oper. Syst. Rev.*, Association for Computing Machinery, New York, NY, USA, v. 43, n. 4, p. 54–59, jan. 2010. ISSN 0163-5980. Disponível em: <https://doi.org/10.1145/1713254.1713267>.

WROCLAWSKI, J. et al. Deterlab and the deter project. In: *The GENI Book*. [S.l.]: Springer, 2016. p. 35–62.