Universidade Federal de Pernambuco

Graduação em Sistemas de Informação

Centro de Informática

2016.2

Principais vulnerabilidades da Internet das coisas e guidelines para resolvê-las

Proposta de Trabalho de Graduação

Aluno:José Durval Carneiro Campello Neto(jdccn@cin.ufpe.br)
Orientador: Kiev Gama(kiev@cin.ufpe.br)

Recife,Setembro de 2016

Sumário

1. Contextualização

A internet das coisas, a partir desse momento será referenciado como IoT, é uma rede global de objetos, “coisas”, unicamente endereçadas baseada em protocolos de comunicação[1]. Ou seja, é a interconexão de veículos, prédios e objetos equipados com sensores,hardware e um software que possibilita que eles consigam coletar, enviar e receber dados[2]. Dados esses que servem para automatizar tarefas do dia a dia, como é o caso do termostado da Nest que aprende seus hábitos e altera a temperatura da sua casa de forma automática de acordo com sua preferência; ter controle remoto da sua casa, como exemplos dezenas de produtos que permitem você abrir a porta da sua garagem através do seu celular[3]. Em geral são produtos que já vêm prontos para o consumidor final, grande parte deles são basicamente dispositivos *plug and play*[4], como exemplo o Xiaomi Gateway. Isto tem com o intuito de tornar a experiência mais prática e fácil para o consumidor final, principalmente por enquanto que a tecnologia não está bastante conhecida do público em geral. Mas esse fato pode ter várias consequências, negativas, no quesito de segurança, por exemplo, câmeras de vigilâncias com senhas padrões de fábricas.

Atualmente IoT tem vários fatores positivos, como: Se encontra no seu auge de popularidade[5]; Se encontra no ponto mais alto no último Gartner Hype Cycle for Emerging Technologies, edição de 2015; Com projeção de atingir seu potencial pleno dentro de um prazo de 5 a 10 anos[6]; Com milhões de dispositivos de IoT já sendo utilizados[7]; E uma projeção de receita de 357 bilhões de dólares, apenas nos Estados unidos, em 2019[8]. Todo esse fatores positivo leva para um alto interesse da indústria em de forma mais rápida novos produtos relacionados a IoT, para suprir a demanda do mercado. Tanto é que empresas mais tradicionais, e startups, estão fazendo altos investimentos em IoT. Um bom indicativo dessa última afirmação é a grande variedade de linhas “smart” em diferentes produtos e o “boom” de startups com foco em IoT[9].

Porém o número de incidentes de segurança envolvendo IoT, acompanha de forma direta a sua popularização. Isso pode ser atribuido ao fato de que, é muito mais fácil, e conveniente, olhar apenas paras as oportunidades em IoT do que paras as ameaças de segurança relacionadas a IoT. Essa fato é bastante preocupante, já que IoT tem uma superfície de ataque grande. E suas falhas de seguranças geralmente são graves, pois o atacante pode conseguir dados sensíveis dos proprietários do dispositivo, além de poder ter acesso e controle ao dispositivo. Esse último cenário é agravado se por exemplo, o dispositivo alvo seja responsável pelo controle das portas, luzes e sistema de som da residência.

2. Objetivo

Este trabalho tem como objetivo principal estudar e analisar as principais vulnerabilidades de IoT, desde sua criação até os dias atuais, e propor guidelines para poder mitigar-las.

3.Cronograma

Atividades	Setembro				Outubro				Novembro				Dezembro			
Preparação da Proposta	X	X														
Estudos sobre principais vulnerabilidades			X	X	X	X										
Estudos sobre mitigação de falhas de segurança				X	X	X	X	X								
Elaboração do Relatório									X	X	X					
Preparação da Defesa												X	X	X		

4.Possíveis avaliadores

- Prof. Vinicius Cardoso Garcia

5.Referências bibliográficas

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol 54, No 15, pp. 2787-2805, 2010.
[2] Internet of Things Global Standards Initiative. Disponível em: < http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx> Acessado em : 12 Setembro de 2016
[3] Best WiFi and Bluetooth Smart Garage Door Openers Disponível em:< http://www.postscapes.com/wifi-garage-door-opener/>

Acessado em : 12 Setembro de 2016
[4] Plug and Play Definition
Disponível em:< http://techterms.com/definition/plugandplay>
Acessado em : 12 Setembro de 2016
[5] Google Trends, Internet of Things Search term
Disponível em:
< https://www.google.com/trends/explore?date=all&q=Internet%20of%20things&hl=en-US>
Acessado em : 15 Setembro de 2016
[6] Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor
Disponível em:< http://www.gartner.com/newsroom/id/3114217>
Acessado em : 12 Setembro de 2016
[7] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015 Disponível em:< http://www.gartner.com/newsroom/id/3165317>
Acessado em : 15 Setembro de 2016
[8] IDC Spending Guide Finds U.S. Organizations Accelerating Their Investment in the Internet of Things as Meaningful Use Cases Find Their Way to Fruition
Disponível em:< http://www.idc.com/getdoc.jsp?containerId=prUS41547916>
Acessado em : 15 Setembro de 2016
[9] Internet of Things Starttups Disponível em:< https://angel.co/internet-of-things>
Acessado em : 15 Setembro de 2016

6.Assinaturas

Kiev Gama
Orientador

José Durval Carneiro Campello Neto
Aluno