Segurança na IoT

Profa. Michelle S. Wangham

Professora na UNIVALI

Assessora de PD&I na RNP

https://www.linkedin.com/in/michelle-wangham/

As “*coisas*” estão seguras na Internet das Coisas?

2014

Researchers have demonstrated that routers, set-top boxes, security cameras, TVs, and even fridges can be hijacked and abused by cybercriminals for various purposes, including sending spam, mining for crypto-currencies, and spreading malware. Medical devices can also be hijacked, and the consequences can be deadly.

On the other hand, experts have also demonstrated that **cars**, **ships**, **airplanes**, **satellites** and even the **sensors used for traffic control systems** can be hacked.

http://news.softpedia.com/news/Everything-Can-Be-Hacked-It-s-Just-a-Matter-of-Time-Until-Things-Get-More-Serious-440322.shtml

NEWS

Thousands of medical devices are vulnerable to hacking, security researchers say

The security flaws put patients' health at risk

2015

By James Niccolai

Deputy News Editor, IDG News Service | SEP 29, 2015 5:50 PM PT

The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's apparently because support teams needed the passwords to service the systems.

http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

Ataques de DDoS

- Setembro/2016: Mirai é identificada: 620Gbps contra o Blog do Brian Krebs

UPDATE

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

By Brad Chacos

Senior Editor, PCWorld | OCT 21, 2016 3:34 PM PT

http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html

E hoje ?

IoT devices more at risk of cyber attack than ever - report

17 Mar 2020

Newsdesk

SHARE:

LinkedIn

Twitter

Facebook

Internet of Things (IoT) devices are one of the fastest-growing emerging technologies in the digital transformation sphere – by the end of 2019, 4.8 billion IoT endpoints were expected to be in use, an increase of 21.5% from 2018, according to Gartner.

But, as with almost all emerging technologies, there comes with it an associated cybersecurity risk.

Unit 42, the threat intelligence team of Palo Alto Networks, recently analysed 1.2 million IoT devices in thousands of physical locations across enterprise IT and healthcare organisations in the United States.

The 2020 Unit 42 IoT Threat Report found the general security posture of IoT devices is declining, leaving organisations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten.

Among the most disturbing discoveries: 98% of all IoT device traffic is unencrypted, exposing personal and confidential data on the network.

E hoje ?

Security Intelligence News

Internet of Threats: IoT Botnets Drive Surge in Network Attacks

April 22, 2021 | By **Dave McMillen** | 6 min read

https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/

As Internet of things (IoT) devices in homes, industrial environments, transportation networks and elsewhere continue to proliferate, so does the attack surface for malicious IoT network attackers. IoT attack activity in 2020 dramatically surpassed the combined volume of IoT activity observed by IBM Security X-Force in 2019.

Shodan | Developers | Book | View All...

SHODAN

Explore | Developer Pricing | Enterprise Access | Contact Us | New to Shodan?

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

The search engine for Power Plants

The search engine for Webcams

The search engine for Refrigerators

The search engine for Buildings

Por que as “coisas” são vulneráveis?

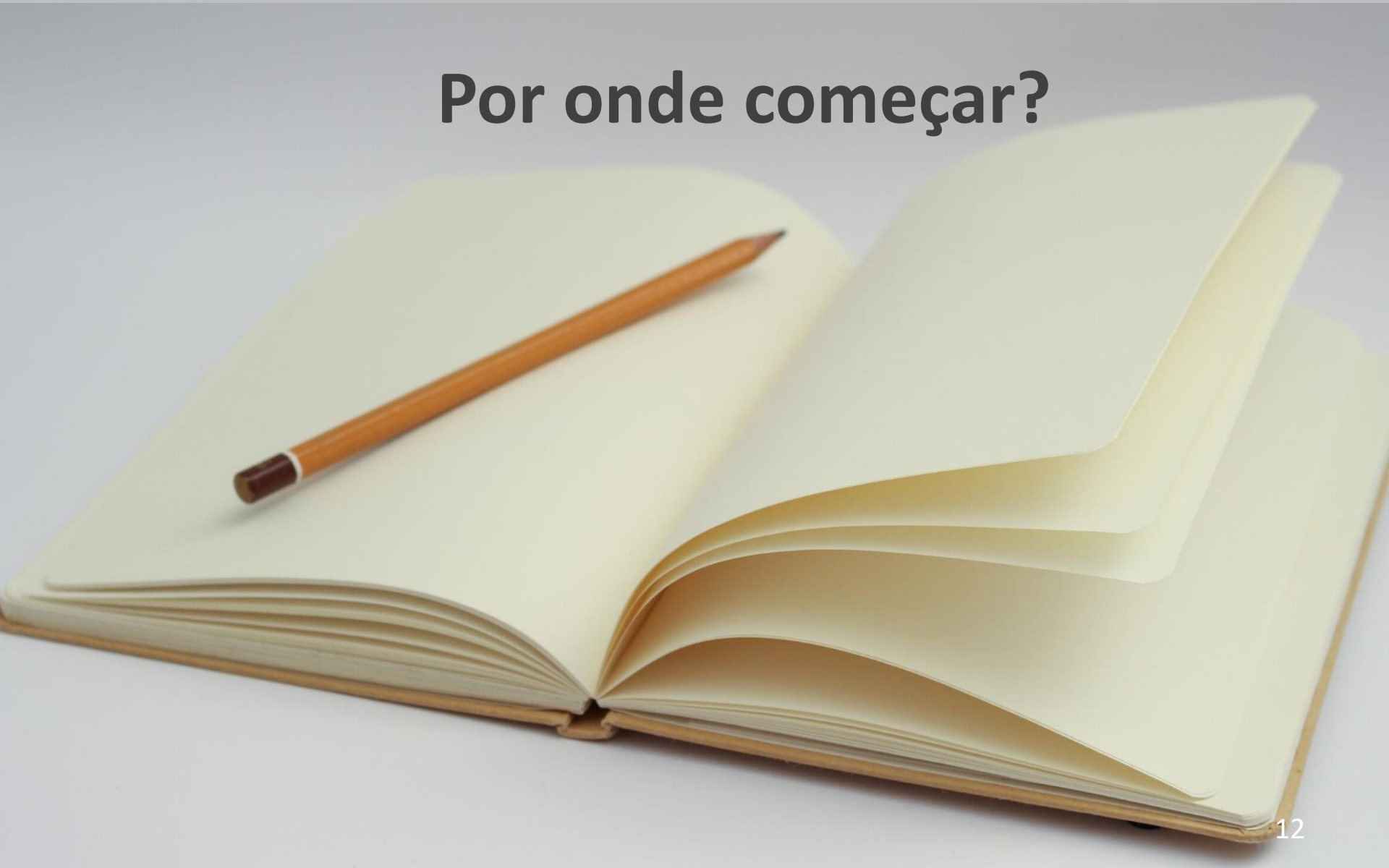
- **Segurança não é prioridade (máquinas industriais)**
- Sistemas operacionais simples: não possuem mecanismos adequados de proteção **e não sofrem atualizações.**
- Inúmeras **vulnerabilidades** nos softwares embarcados (botnets, veículos, *smartphones*, dispositivos médicos, centrais de alarmes, sistema aquecimento, sistemas elétricos)
- Dificuldades para atualizações e aplicações de ***patches* de segurança**
- Desejo das empresas fabricantes de equipamentos de manter *backdoors*
- Soluções **sem criptografia** ou protocolos mal implementados
- Dispositivos **expostos** diretamente na Internet
- **Falta ou falha de mecanismos de autenticação**

Segurança e Privacidade na IoT

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Legalidade
- *Proteção de dados pessoais*

- I1 Weak Guessable, or Hardcoded Passwords
- I2 Insecure Network Services
- I3 Insecure Ecosystem Interfaces
- I4 Lack of Secure Update Mechanism
- I5 Use of Insecure or Outdated Components
- I6 Insufficient Privacy Protection
- I7 Insecure Data Transfer and Storage
- I8 Lack of Device Management
- I9 Insecure Default Settings
- I10 Lack of Physical Hardening

Por onde começar?



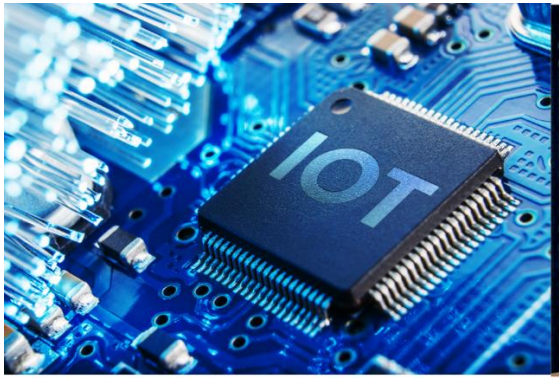
Na IoT, passado se repete...

- Garantir que senhas fortes são requeridas
- Implementar MFA quando possível
- Garantir que as credenciais são protegidas
- Garantir que os mecanismos de recuperação de senhas são seguros
- Garantir que a re-autenticação é requeridade para características sensíveis (autenticação contínua)
- Usar **IAM (autenticação de usuários e de dispositivos)**

Autenticação de Dispositivos

- Criptografia simétrica (AES)
- Certificados digitais (cripto assimétrica)
- *Tokens* assinados com chaves compartilhadas (Azure IoT)
- Criptografia assimétricas alternativas (*certificateless* e *IBC)*
- Criptografia leve
  - Encriptação **simétrica**: *LS Designs, redes modernas de Feistel e Adição-Rotação-Soma (ARX), PRESENT*
  - **MACs** curtos usando SipHash ou **assinaturas digitais** construídas a partir de *hashs* com entradas curtas (não resistentes a colisão) ou BLAKE2.
  - Criptografia de curvas elípticas (**ECC**)

Contexto Atual



Notícias Recentes

- Estudo Global Cyberattack Trends da SonicWall
  - Ataques de malware a dispositivos IoT aumentam 66% (*ransomware* e *cryptojacking*)[1]
  - 6 em cada 10 (57%) dispositivos IoT são vulneráveis [1]
- Diretor de Fintech teve conversas gravadas por um alto falante inteligente
- Ataques a dispositivos IoT em redes domésticas – alvo redes corporativas
- Ataque empresa de oleoduto nos EUA (*ransomware*)

Boas Práticas

Boas práticas

- Autenticação robusta (IAM) – *Zero Trust Identity*
- Aumentar a visibilidade da IoT
- Protocolos seguros (***end-to-end security***)
- Segurança em **camadas**
- **Segmentar TI e TO // ISP rede domestica e ISP Home office**
- Detecção e Resposta Estendida (**XDR**)
- Gestão de vulnerabilidades e de **riscos**
- **Testes** de software e Testes de invasão
- Novos mecanismos: uso de *machine learning* e *deep learning* (predição e detecção)
- **Pesquisa Experimental** (*testbed* e simulação)

Segurança na IoT

Profa. Michelle S. Wangham

Professora na UNIVALI

Assessora de PD&I na RNP

https://www.linkedin.com/in/michelle-wangham/

Projeto de 5 anos

MENTORED

Da Modelagem à Experimentação
Predizendo e detectando ataques DDoS e zero-day

FAPESP

MCTIC

cgi.br
Comitê Gestor da Internet no Brasil

Visão Geral: Arcabouço de Soluções