Internet das Coisas:
Risco associados à adoção de equipamentos IoT em um cenário de ameaças

Alex Simonetti Abreu

Arquiteto de Software

THE DEVELOPER'S CONFERENCE

THE DEVELOPER'S CONFERENCE

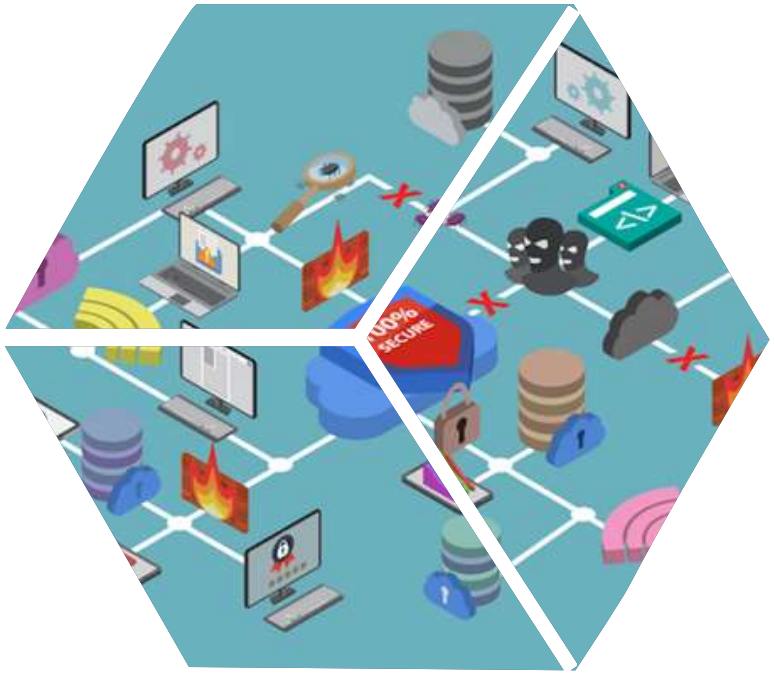
01

contexto

THE DEVELOPER'S CONFERENCE

- Cada vez mais onipresente
- Impacto global de US$ 11 trilhões até 2025
- 26 bilhões de dispositivos até 2020 (Gartner Group)
- Um dos fatores motivadores da 4ª Revolução Industrial
- Conceito controverso e ainda em discussão
- Em passo acelerado de evolução
- Potencialidades ainda não mapeadas

THE DEVELOPER'S CONFERENCE



02

TCP/IP: uma breve história

- Publicado em 1974, e adotado oficialmente na ARPANET em 1981
- Inerentemente insegura: pensava-se em segurança por confiança
- Não há garantia de autenticação das partes
- Não existe um modelo padronizado do protocolo: cada um implementa como quer
- Quase toda melhoria de segurança depende de métodos de criptografia
- Sujeito a *bugs*, até mesmo na criptografia

THE DEVELOPER'S CONFERENCE

03

segurança da informação

- Confidencialidade: apenas aos autorizados
- Integridade: sem alterações indesejadas
- Disponibilidade: disponível quando requisitada
- Irretratabilidade: não-repúdio
- Autenticação: identidade dos interlocutores

THE DEVELOPER'S CONFERENCE

04

ameaças comuns

THE DEVELOPER'S CONFERENCE

- Disfarce (imitação)
- *Man-in-the-middle*
- DoS, DDoS, PDoS

- Malware
- Zumbis
- Botnets

05

afinal, o que é Internet das Coisas?

Internet das Coisas: o que é

Kevin Ashton, Inglaterra, 1999 → RFID

Academia: diversas definições

Weber (2011): apenas RFID, para troca de mensagens

Li e Zhou (2011) : RFID + sensores + GPS + inteligência

Huang e Hua (2017): qualquer dispositivo com internet

Atzori, Iera e Morabito (2010): mais amplo, cooperativo

THE DEVELOPER'S CONFERENCE

Não existe uma definição clara, objetiva, e amplamente aceita – ou universal - do que seja Internet das Coisas.

Tudo que se aceita universalmente é que mais cedo ou mais tarde será um elemento onipresente em nosso mundo.

RISCO: indefinição do que é IoT

AMEACA: tributações, legislações divergentes

Internet das Coisas: o que é

Governos: diversas definições

União Europeia: ainda busca, mas antecipa com uma referência a uma rede distribuída de objetos físicos interconectados

EUA: “Não existe definição amplamente aceita”; exclui celulares, tablets e computadores

Brasil: Plano Nacional de IoT do MCTIC + Anatel, aceita pelo UIT em 2019 como proposta de padronização para os ~190 países e 700+ empresas membros.

Indústria: diversas definições

IEEE: aceita que existem definições diferentes
ITU : similar à de Atzori, Iera e Morabito (2010)

Chegaremos a um momento onde não será possível ignorar a adoção de dispositivos IoT nos processos industriais. No entanto, estamos em um momento onde existe uma multitude de modelos de padrões propostos e nenhum oficialmente regulamentado ou adotado voluntariamente como padrão pelo mercado.

Limitações

THE DEVELOPER'S CONFERENCE

Bateria: autonomia limitada

Processamento

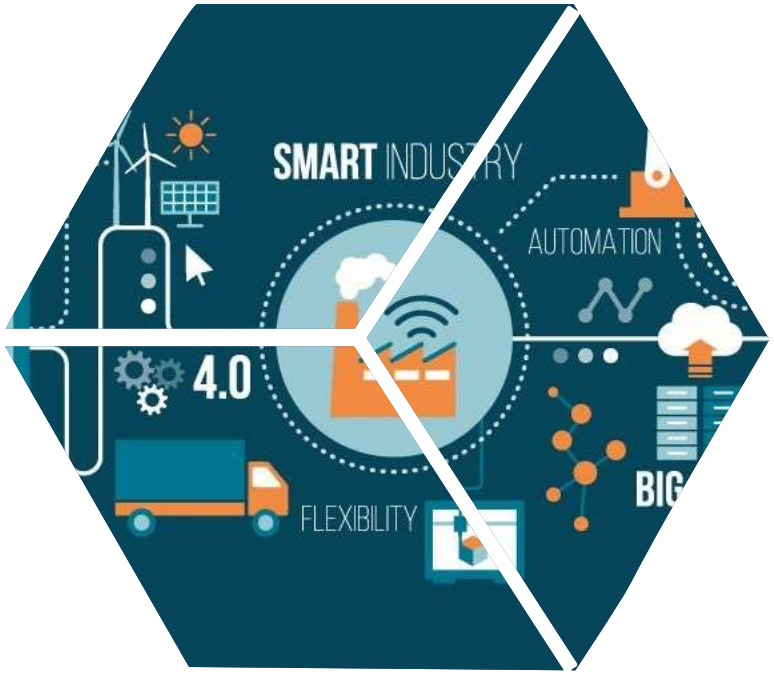
Memória

Capacidade de implementar um stack de conectividade completo e seguro

Ficam fisicamente desacompanhados a maior parte do tempo

Redes wi-fi são mais suscetíveis a ataques

THE DEVELOPER'S CONFERENCE



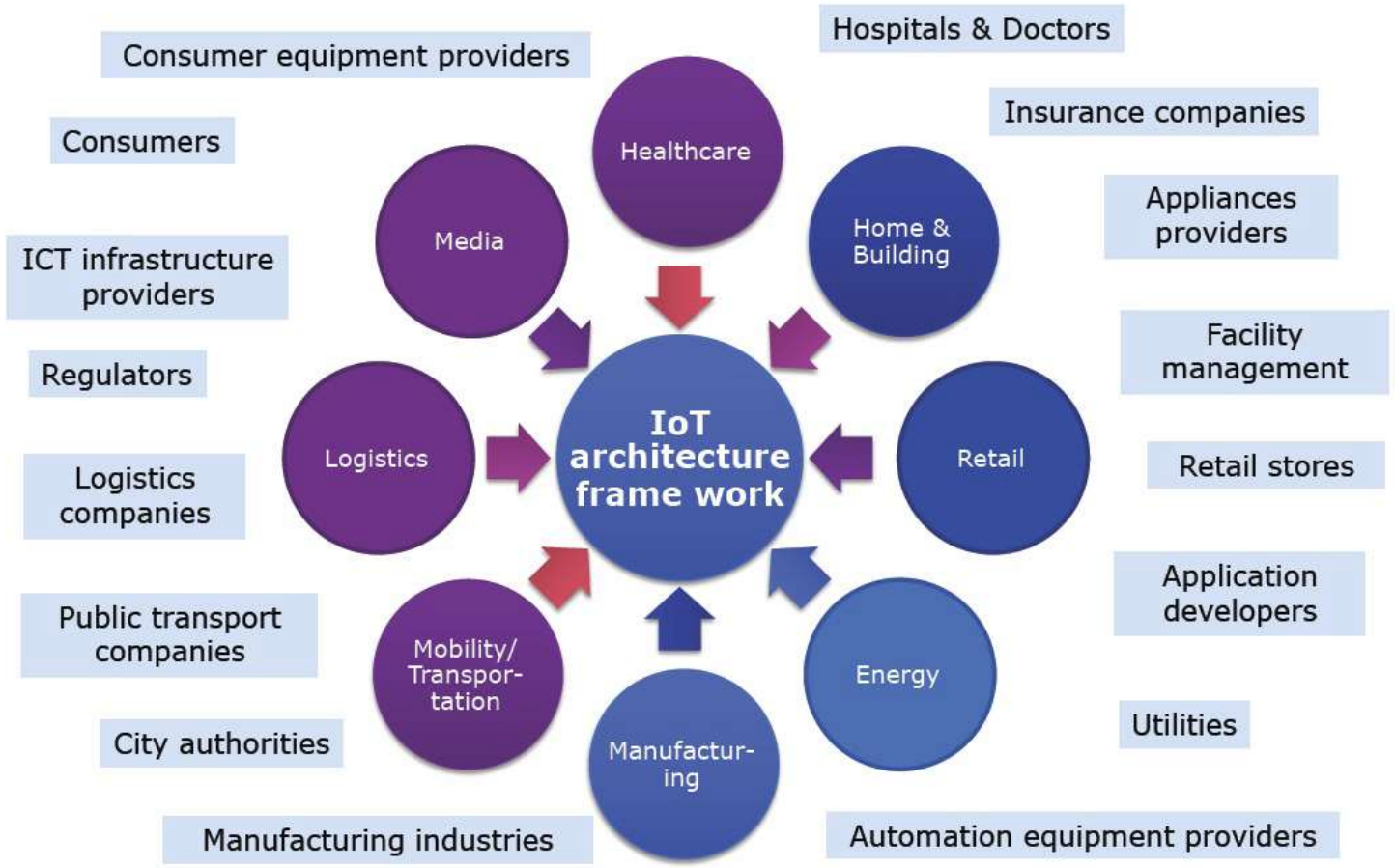
06

aplicações

- Cidades inteligentes (Smart cities)
- Domótica (evolução da automação residencial)
- e-Health ou IoMT: saúde
- IIoT: indústria
- Cybermanufacturing
- e-Wear (tecidos e roupas inteligentes)
- Pecuária inteligente

Por falta de definição padronizada, cada segmento de mercado busca sua própria definição e designação para IoT

Internet das Coisas: aplicações



Fonte: *Towards a Definition of the Internet of Things (IoT)*. Minerva, Biru e Rotondi (2015, p.12)

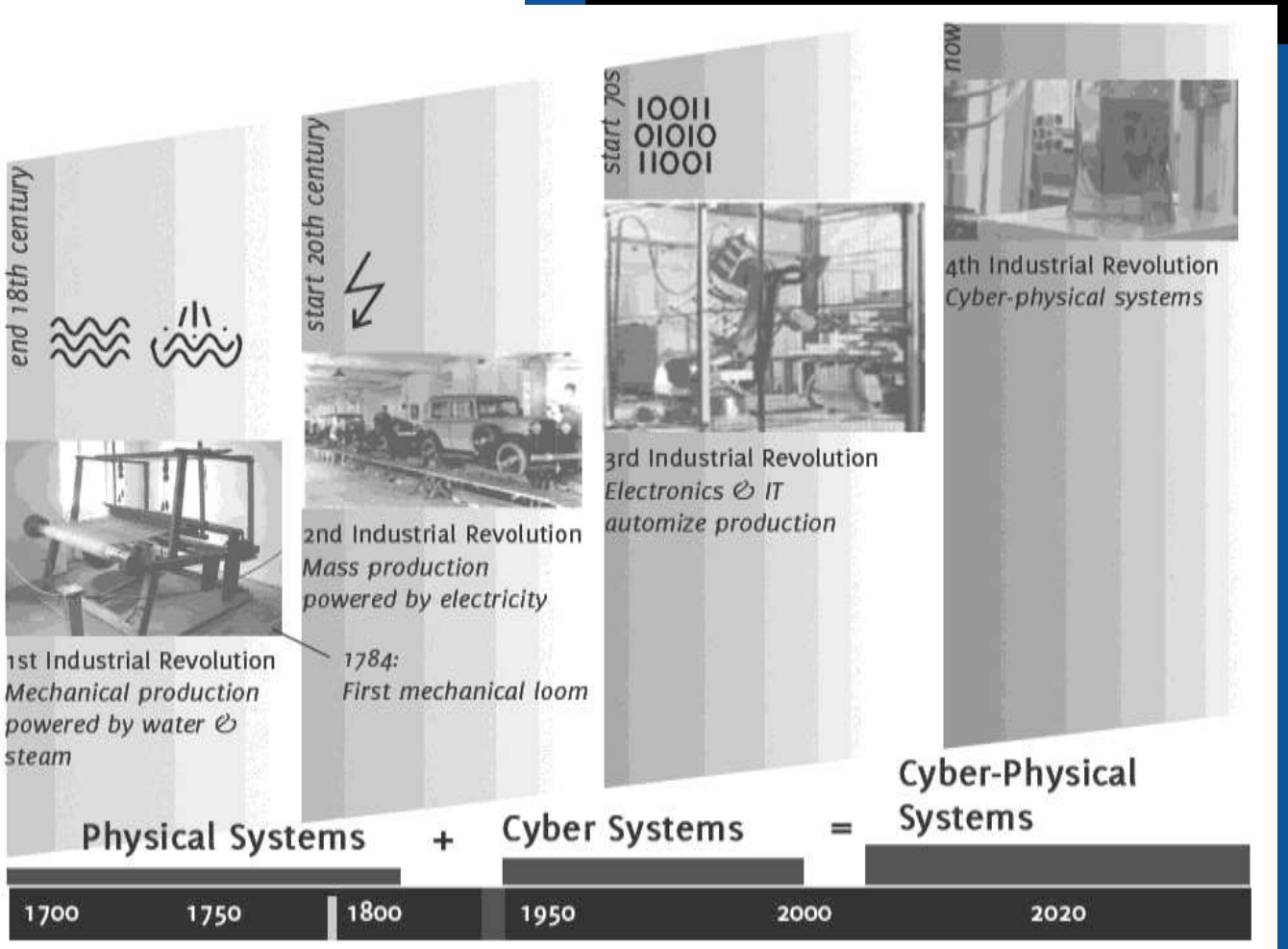
CPS: Sistemas Ciber-Físicos

THE DEVELOPER'S CONFERENCE

- Especialização de IoT: coleta, processamento e transmissão de dados
- Composto de CPOs: Objetos Ciber-Físicos
- Todos os CPOs estão dentro da fronteira do CPS
- Há cooperação entre os CPOs
- Há um servidor na retaguarda (ou nuvem), responsável por armazenar e processar as informações coletadas pelos sensores
- Retroalimentação (*feedback loop*)
- O CPS está conectado à internet. Os CPOs não.
- Exemplos: Indústria 4.0, domótica, Smart cities

I40: INDUSTRIA 4.0

- 1ª Revolução Industrial:
  1784. Máquinas hidráulicas e movidas a vapor + ferrovias
- 2ª Revolução Industrial:
  Início séc. XX. Eletricidade + esteiras transportadoras + linhas de montagem = produção em massa
- 3ª Revolução Industrial:
  Anos 70. sistemas eletrônicos + TI = automação da produção
- 4ª Revolução Industrial:
  Em andamento. Internet móvel + IoT/CPS + big data + IA + computação ubíqua.



THE DEVELOPER'S CONFERENCE

07

casos de ataques

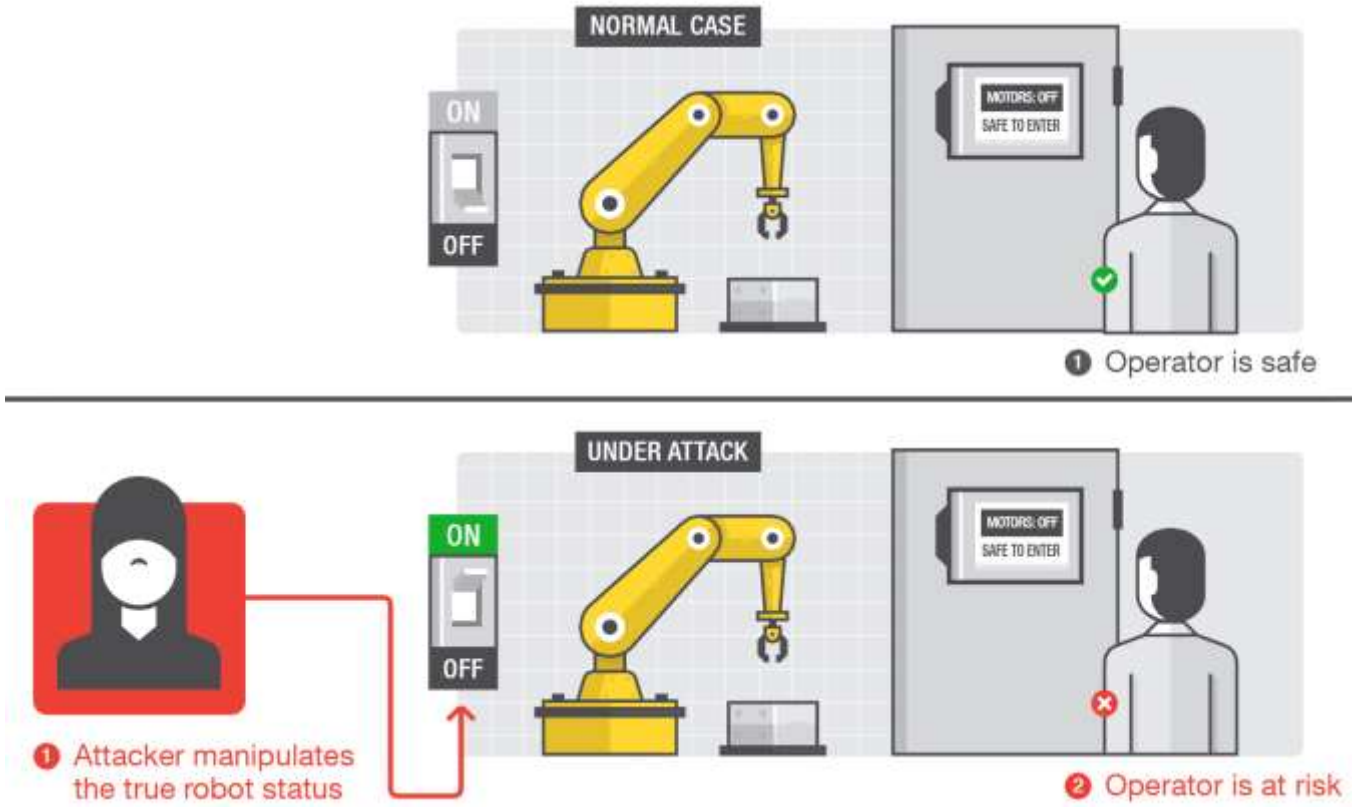
Casos de Ataques

- ~~**Shodan**~~: O “Google” da IoT → censys.io, zoomeye.org
- **BrickerBot**: ataca Telnet, causa **P**DoS
- 2013, botnet de 100k TVs e geladeiras IoT enviou 750k e-mails
- **TOCTTOU**: SmartTVs Samsung
- Incidente **FOSCAM**
- **Mirai**: um dos 3 maiores DDoS da história, em 20/10/16 (DynDNS). Vários ataques posteriores (Deustche Telekom, TalkTalk, OVH). Ataque à OVH usou botnet de 152.000 dispositivos e teve picos de 1Tbps. Atualmente OpenSource.
- **Hajime**: controle distribuído. >300k dispositivos. Latente.

As ferramentas de busca de dispositivos, como o Shodan e o Censys, facilitam encontrar dispositivos IoT vulneráveis e expostos.

Quando combinados com ferramentas como THC Hydra, vulnerabilidades podem ser facilmente exploradas.

Risco: equipamentos industriais



THE DEVELOPER'S CONFERENCE

Um equipamento industrial comprometido pode envolver mais do que prejuízo financeiro: pode colocar em risco a vida de seres humanos.

A Universidade Politécnica de Milão e a Trend Micro conseguiram mapear robôs industriais diretamente conectados `a internet ou redes wi-fi inseguras (para, por exemplo, fazer um "call home" para dados de telemetria e produção).

CaaS – Crime as a Service

EUROPOL: *Internet Organized Crime Threat Assessment*, 2017

Alusão a termos comuns da indústria (**SaaS, IaaS, PaaS**)

Botnets passam a ser infraestruturas que podem ser alugadas para **ciberterrorismo**, **hacktivismo**, **hijacking** e outras atividades cibernéticas criminosas.

WikiLeaks, Vault7 e a CIA

THE DEVELOPER'S CONFERENCE

- **Ataques à privacidade**
- **Mudança de paradigma** da coleta de inteligência:
  - Pós-fato → Tempo real
  - Texto (eventualmente áudio) → Qualquer formato
  - Alvos colaterais → Alvos pontuais
- Várias das ferramentas **utilizam dispositivos IoT**
  - Weeping Angel: televisores Samsung
  - Pterodactyl: dispositivos (IoT ou não) que usam Linux / Android
  - Sontaram: smartphones
  - MaddeningWhispers: acesso remoto em sistemas móveis e embarcados que usam o Vanguard
  - HarpyEagle: IoT da Apple, como Airport Extreme e Time Capsule

THE DEVELOPER'S CONFERENCE

08

estudos e conclusões

Estudos de Melhoria de IoT

THE DEVELOPER'S CONFERENCE

- A maior parte dos estudos em andamento visa melhorar a segurança ou privacidade dos dispositivos IoT
- Criptografia
- Os estudos sugerem que seus achados sejam adotados como padrão pelo mercado

Conclusões

THE DEVELOPER'S CONFERENCE

- Não há uma definição padronizada para IoT → Problemas para comércio exterior
- Depende de TCP/IP que é inerentemente inseguro
- Dispositivos IoT [ainda] são uma ameaça a eles e a todo o ecossistema da internet
- Dezenas de padrões propostos, nenhum oficialmente
- Adotar um modelo atualmente pode causar perda do investimento no futuro (ex.: Betamax, HD-DVD)
- A situação de leis e taxas no Brasil ainda é volátil

Conheca seu risco

THE DEVELOPER'S CONFERENCE

- Faça análise de seu parque de equipamentos IoT instalados
- “Hackers do bem” (white hat hackers)
- Scanners de vulnerabilidade
- Atualizações de firmware em ambiente controlado
- Proteja a rede de fora para dentro (borda para equipamentos)

THE DEVELOPER'S CONFERENCE

"The nice thing about standards is that you have so many to choose from; furthermore, if you do not like any of them, you can just wait for next year's model."

Andrew S. Tanenbaum

"Computer Networks", 1981.

THE DEVELOPER'S CONFERENCE

Obrigado!

Alex Simonetti Abreu

simonetti@gmail.com

https://www.linkedin.com/in/alexsimonetti/