Internet das Coisas (IoT)

Prof. Dr. Dilermando Piva Jr.
Fatec Indaiatuba

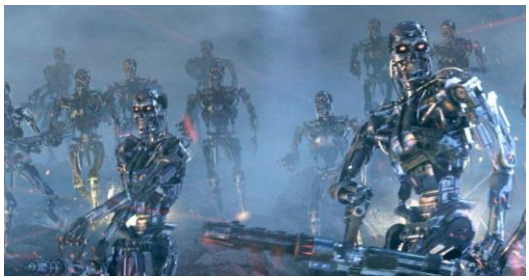
The Internet of Things (IoT)
Internet das Coisas ou de Tudo

O que IoT?

- A **Internet das Coisas** (IoT) é a rede de objetos físicos - dispositivos, veículos, edifícios e outros itens incorporados em aparelhos eletrônicos, software, sensores e conectividade de rede - que permite que esses objetos coletem e troquem dados.

Vários nomes... um Conceito

- M2M (Machine to Machine)
- "Internet of Everything" (Cisco Systems)
- "World Size Web" (Bruce Schneier)
- "Skynet" (Filme: O exterminador do futuro)



Onde está a IoT?

Em TODOS os lugares !!
It's everywhere !!

Aparelhos Inteligentes

Tecnologias Usáveis Wearable Tech

Cuidados com a Saúde

8

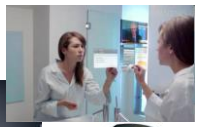
Os dispositivos com sensores estão se tornando amplamente acessíveis

- Dispositivos programáveis
- Ferramentas e aparelhos de prateleira

9

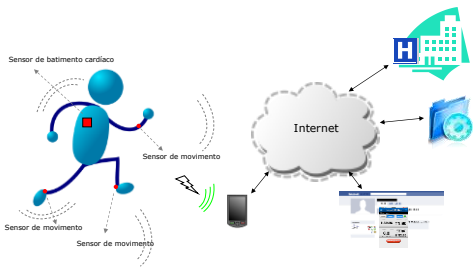
Mais “coisas” estão sendo conectadas

Dispositivos domésticos
Infraestrutura pública e privada
Cuidados com a saúde
…



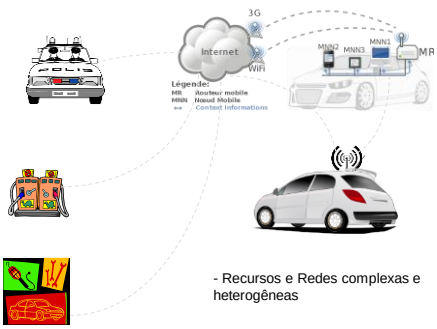
10

Pessoas conectadas a Coisas



11

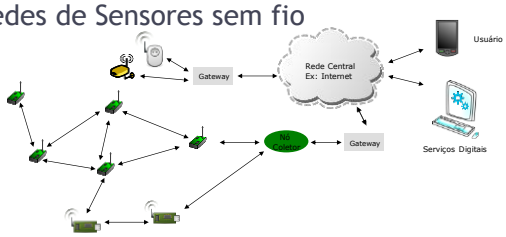
Coisas conectadas a Coisas



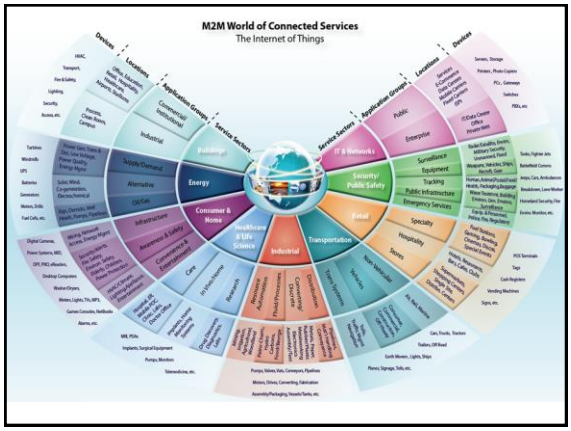
- Recursos e Redes complexas e heterogêneas

12

Wireless Sensor Networks (WSN)
Redes de Sensores sem fio

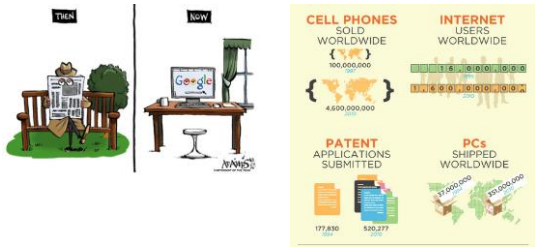


- As redes geralmente trabalham com dispositivos de baixa potência
- Consiste em um ou mais sensors… podem ser sensors (ou atuadores) de diferentes tipos



15

Internet – antes e hoje



Onde está (ou estará) a IoT?

Na Faculdade...

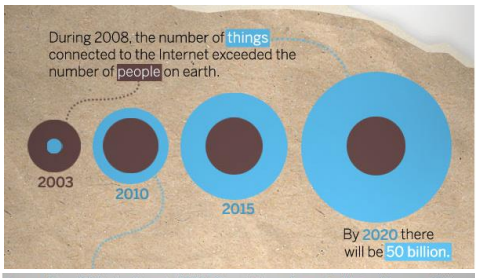
The Smart *Internet of Things* School

O Mercado da IoT

- Desde 2015, 20 bilhões de unidades de IoT
- Expectativa de crescimento até 2020: 50 bilhões de dispositivos com IoT
- A expectativa de receita com IoT até 2020 é de $15 trilhões

19

"Coisas" conectadas a Internet

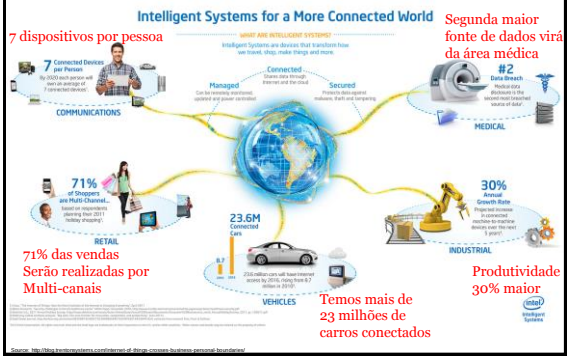


Sources: Cisco IBSG, Jim Cicconi, AT&T , Steve Leibson, Computer History Museum, CNN, University of Michigan, Fraunhofer

cisco

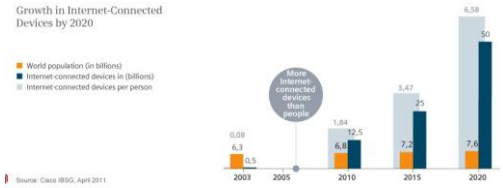
19

20



21

Dispositivos Conectados à Internet



Source: Siemens, http://www.siemens.com/innovation/apps/pof_microsite/_pof-fall-2012/_html_en/facts-and-forecasts-growth-market-of-the-future.html

Por quê se preocupar com IoT?

- É apenas outro computador, certo?
  - Os mesmos problemas que temos como o controle de acesso, gerenciamento de vulnerabilidade, monitoramento etc.
  - Imagine sua rede com mais de 1 milhão de novos dispositivos
  - Qualquer dispositivo com capacidade de conexão terá a rede como apoio.

Qual será o risco adicionado com a IoT?

- Os dispositivos altamente portáteis são capturados durante as varreduras de vulnerabilidade?
- Onde está o seu perímetro de rede?
- Os dispositivos dos clientes são usados em áreas – como hospitalares – onde a confiabilidade é crítica?
- Os usuários instalam softwares de gerenciamento de dispositivos em outros computadores? Esses são outros vetores de ataque?

Qual será o risco adicionado com a IoT?

- Os dispositivos altamente portáteis são capturados durante as varreduras de vulnerabilidade?
- Onde está o seu perímetro de rede?
- Os dispositivos dos clientes são usados em áreas – como hospitalares – onde a confiabilidade é crítica?
- Os usuários instalam softwares de gerenciamento de dispositivos em outros computadores? Esses são outros vetores de ataque?

SEGURANÇA

Atacando a IoT

- Credenciais padrão, fracas e codificadas
- Difícil de atualizar firmware e SO
- Falta de suporte de fornecedores para reparar vulnerabilidades
- Interfaces Web vulneráveis (injeção SQL, XSS
- Erros de Codificação (overflow de buffer)
- Protocolo de texto claro e portas abertas desnecessárias
- DoS / DDoS
- Roubo físico e adulteração

Além da Segurança...

- Análise de dados (Big Data)
  - MapReduce (modelo de programação para suportar computação paralela – framework Google)
  - Conjunto de itens frequentes
  - Similaridade
  - Clustering
  - Redução de Dimensões
  - Dados de transmissão
- Conectividade (IPv6, WSN, Bluetooth/ZigBee e Wifi/LTE)
- Dispositivos e Plataformas (Sistemas Móveis, Vestíveis, Energia reutilizável ...)

Estudo de Caso: Trane

- As vulnerabilidades do termostato conectado detectadas pelo grupo Talos da Cisco permitiram o suporte na rede
- 12 meses para publicar correções para 2 vulnerabilidades
- 21 meses para publicar correção para 1 vulnerabilidade
- Os proprietários de dispositivos podem não estar cientes das correções ou ter a habilidade de instalar atualizações

Estudo de Caso: Lições Aprendidas

- Todo o software pode conter vulnerabilidades
- Público não informado por meses
- Os fornecedores podem atrasar ou ignorar problemas
- Ciclo de vida do produto e fim de suporte
- Os dispositivos IoT podem não se dimensionar em grandes ambientes

Recomendações...

Acomodar a IoT com práticas já existentes

- Políticas, Procedimentos e Padrões
- Treinamento de conscientização
- Gerenciamento de riscos
- Gerenciamento de Vulnerabilidade
- Forense Computacional

Mais Recomendações...

- Plano para o Crescimento da IoT:
  - Tipos adicionais de registro, armazenamento de log: você consegue encontrar a agulha no palheiro?
  - Aumento do tráfego de rede: seu firewall / IDS / IPS será compatível e continuará?
  - Aumento da demanda por endereços IP tanto IPv4 quanto IPv6
  - Maior complexidade de rede - esses dispositivos devem ser isolados ou segmentados?


Information Security
References
http://www.utsystem.edu/offices/board-regents/uts165-standards
https://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx
https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf
http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html
http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability/#
http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about
https://thenewstack.io/tutorial-prototyping-a-sensor-node-and-iot-gateway-with-arduino-and-raspberry-pi-part-1
http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf
http://blog.talosintel.com/2016/02/trane-iot.html
http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/
http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/