ISOC PT

IGF Aveiro

OUT 2018

Sessão:

Governação, Confiança, Privacidade e Desafios na era da IoT

ISOC PT

IGF Aveiro

OUT 2018

Confiança, Segurança e Privacidade na IoT:

Situação Atual, Desafios e Linhas de Ação

Henrique Domingos

ISOC PT

FCT/UNL, Nova Lincs Research Center

ISOC
Internet Society

ISOC
Internet Society

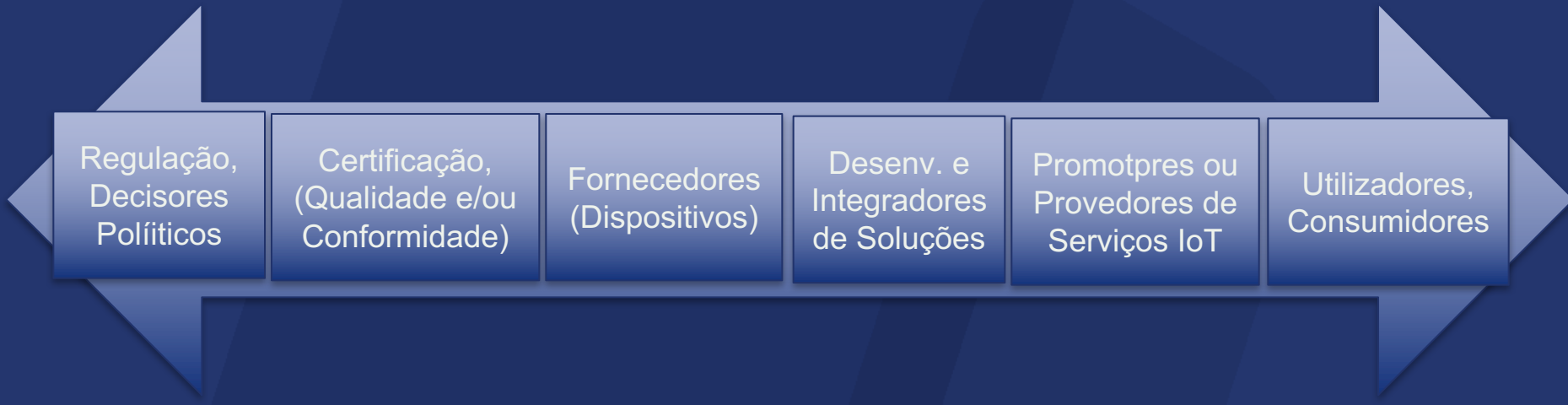
Organização internacional, independente e sem fins lucrativos, que promove o desenvolvimento e evolução da INTERNET de forma ABERTA, INCLUSIVA, SEGURA, NEUTRA e CONFIÁVEL, para toda a gente !

ISOC
Internet Society

Perspectiva e Iniciativas ISOC na área da IoT

A IoT (com I) …
com desenvolvimento natural
e sustentável na Internet

ISOC: Abertura e Colaboração
Num quadro de Debate e de Responsabilidades (verdadeiramente) Multi-Stakeholder



- Normalização e Boas Práticas
- Modelos de negócio vs Modelo de Responsabilidade
- Ética e Legalidade
- Equilíbrio justo de interesses e agendas

ISOC: Articulação em várias Dimensões

Debate, Diagnósticos, Políticas,
Implicações Sociais,
Responsabilidade Social

Especialização dos
Problemas:
Informação, *Awareness*

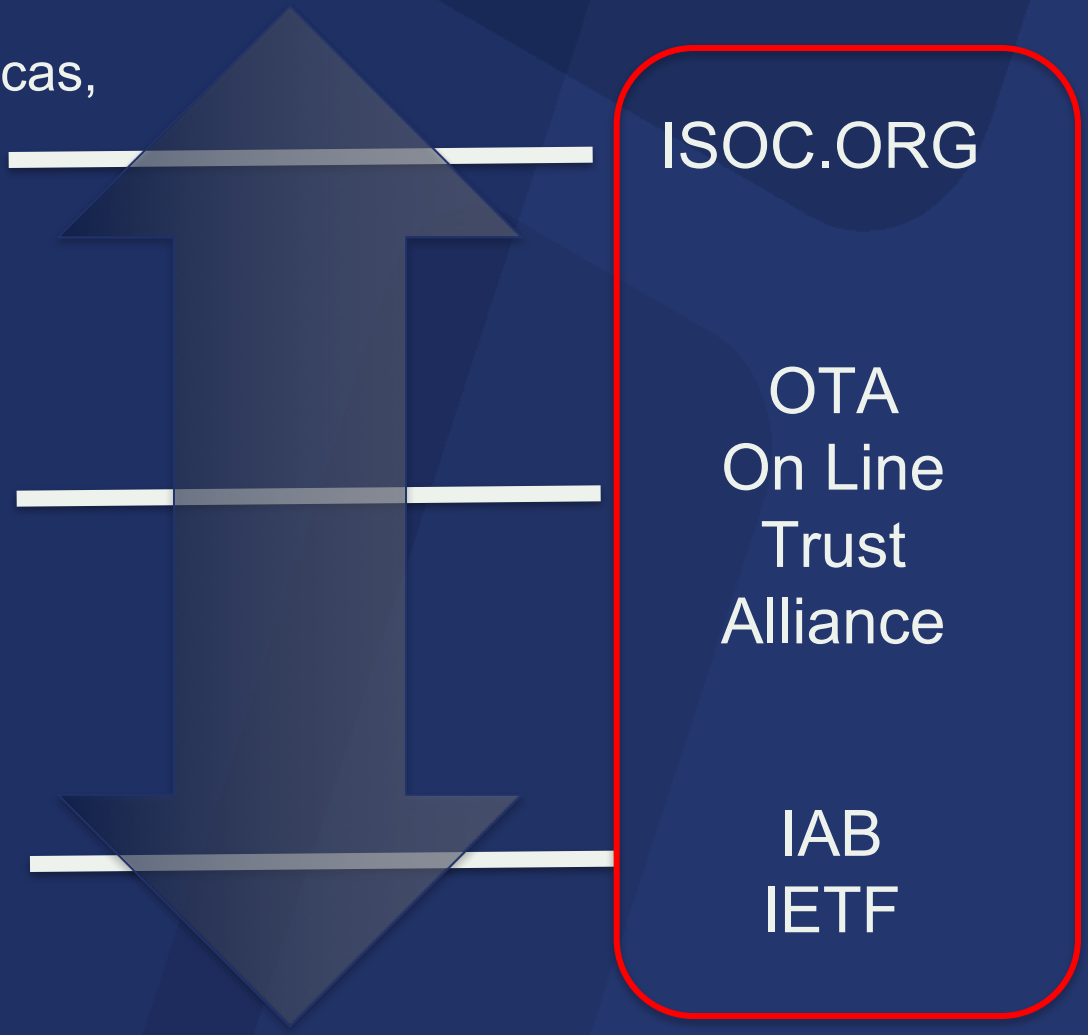
Agendas de Ação
Implicações Técnicas,
Tecnologias de Referência

ISOC: Articulação *Multi-Stakeholder* nas várias dimensões de intervenção

Debate, Diagnósticos, Políticas,
Implicações Sociais,
Responsabilidade Social

Especialização dos
Problemas:
Informação, *Awareness*

Agendas de Ação
Implicações Técnicas,
Tecnologias de Referência



Internet Society

ISOC.PT

OTA Online Trust Alliance
an Internet Society initiative

OTA IoT Trust Framework

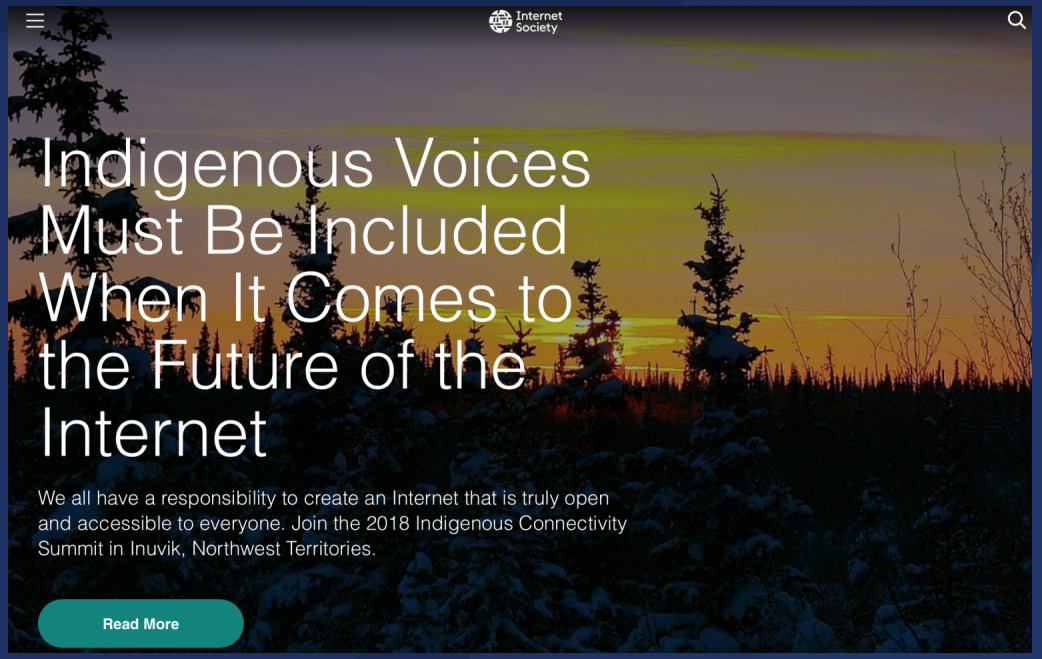
IAB Internet Architecture Board

IETF

IETF Areas and Working Groups

IETF IoT
Internet of Things
Directorate
(iotdir)

www.isoc.org



www.isoc.pt

www.isoc.org

www.isoc.pt

> internetsociety.org/ota/

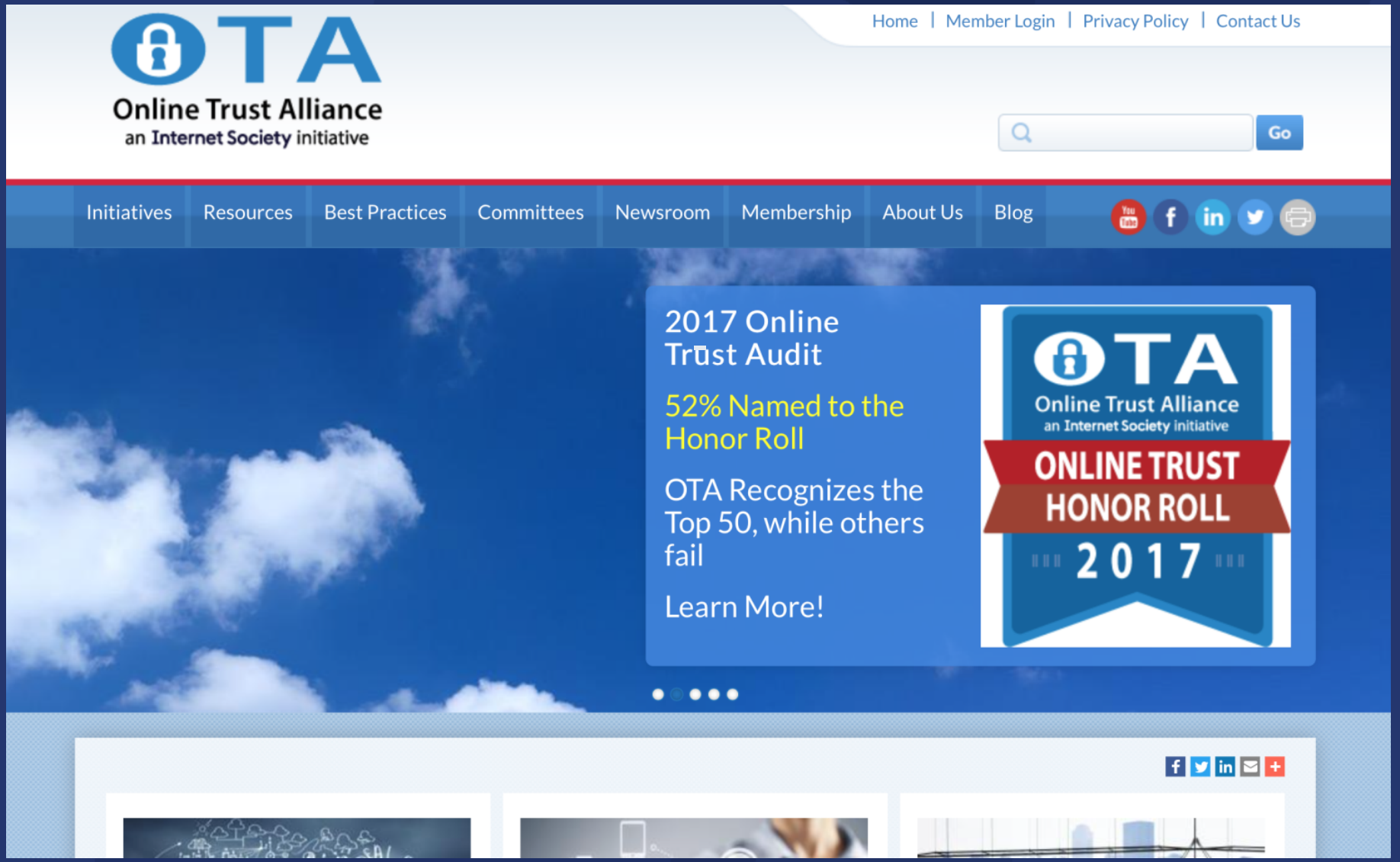
The Online Trust Alliance (OTA) is an Internet Society initiative. OTA's mission is to enhance online trust, user empowerment, and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, ethical privacy practices, and data stewardship.

OTA
Online Trust Alliance
an Internet Society initiative

OTA goals include:

- Educating businesses, policy makers, and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.
- Supporting collaborative public-private partnerships, benchmark reporting,

> OTA: otalliance.org



> OTA IoT: otalliance.org/initiatives/internet-things

- IoT Trust Framework v2.5

Initiatives | Resources | Best Practices | Committees | Newsroom | Membership | About Us | Blog

Home › Initiatives › Internet of Things

Internet of Things

IoT Vision | Consumer | Industry

Vision - An IoT ecosystem built on trust and innovation by prioritizing safety, privacy, and security

The Internet of Things (IoT) offer consumers, businesses, and governments across the globe countless benefits. As is true with most emerging technology, however, there remain some significant challenges. OTA believes that through **leadership, innovation**, and **collaboration,** we can overcome these challenges and create a safer and more trustworthy connected world. This requires a shared responsibility including industry embracing security and privacy by design and adopting responsible privacy practices.

Key Resources

- About the OTA's Internet of Things (IoT) Trust Framework
- Internet of Things (IoT) Trust Framework v2.5
- Enterprise IoT Security Checklist
- Smart Home Checklist, Advice for Buyers, Sellers & Renters
- Securing the Internet of Things: A Collaborative & Shared Responsibility
- IoT Vision for the Future White Paper

Upcoming Events | News

OTA Blog | Newsletters

Thu, Oct 4, 2018

National Cybersecurity Awareness Month = International IoT Security and Privacy Month

October is National Cybersecurity Awareness Month, and as part of our work with the Internet Society and Internet of Things (IoT) campaign, we think October also deserves another label… *International IoT Security and Privacy Month*. There are a number of significant activities and developments related to security and privacy.

Thu, Aug 23, 2018

Announcing the Online Trust Audit & Honor Roll Methodology for 2018

Later this year, we'll publish the 10th annual Online Trust Audit & Honor Roll, which promotes responsible online privacy and data security practices and recognizes leaders in the public and private sectors who have embraced them. This morning, we released the methodology we'll use for this year's audit.

Thu, May 10, 2018

Nest Alert: Protection From Pwned*

> IAB/IETF: www.ietf.org/topics/iot/

The Internet of Things

The Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices.

The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development will usher in more machine-to-machine communication using the Internet with no human user actively involved.

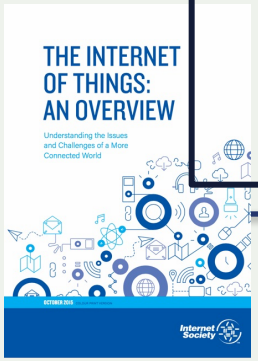
IoT is a very rapidly growing area of technology and connects with number of other emerging technologies. Several IETF working groups, spanning multiple Areas are developing protocols that are directly relevant to the IoT. These protocols are used by a variety of companies, as well as IoT standards organizations and alliances, to build and specify interoperable systems. Due to the distributed nature of IoT protocol development and use, there is often need for coordination across different groups working on IoT.

IoT como Terminologia, Conceito e Paradigma
ISOC, OTA (*)

Ecossistema permeado de dispositivos (sensores, actuadores, computadores) e serviços (SW, Processos), para colectar, trocar e processar dados

Capacidade de processamento com **reação e adaptação dinâmica no contexto ciberfísico** em que se insere e em que opera

- Habilitação para "**Infraestruturas ciber-físicas inteligentes**" visando a **melhoria da qualidade com automatização dos processos de decisão**, para provisionamento de diferentes tipos aplicações, serviços ou modelos de negócio
- **Evolução potenciada pelos princípios e propriedades que caracterizam as fundações da Internet (neutralidade, confiabilidade e abertura das funções CORE) para operação da periferia (EDGE)**



(*) The Internet of Things – An Overview
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

IoT como Conceito, Paradigma ...
... mas com diferentes visões e interesses

Diferentes definições (ISOC, EU, ENISA, ITU-T, GSMA, etc)

Mas também há as visões de diversos intervenientes:

... Alguns conceitos similares, algumas preocupações gerais comuns

... **mas terminologias, ênfases, interesses, heterogeneidades e agendas de prioridades mais ou menos diferenciadas e que podem promover fragmentação, entrincheiramentos e bloqueamentos, dificultando as necessárias convergências.**

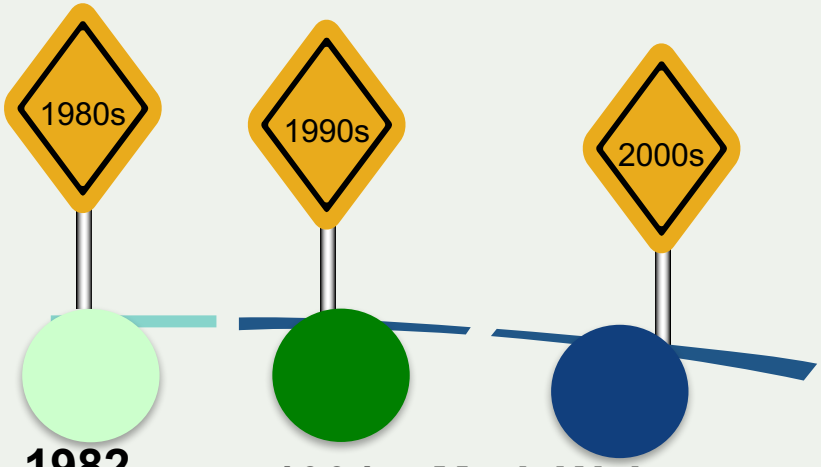
Os perigos de visões "uni-stakholder"

Internet ... IoT

1980s ... 2000 ...

Internet … IoT

O potencial da interoperabilidade da Internet e da pilha TCP/IP ?)



1982
CMU
Internet
Coke
Machine

1991 – Mark Weiser,
XEROX Parc,
Ubiquitous Computing

The Computer for the 21st Century, Scientific America, Sep/1991

1991 ...
Comunidades (Investigação):
UBIquitous Computing
PERVASIVE Computing

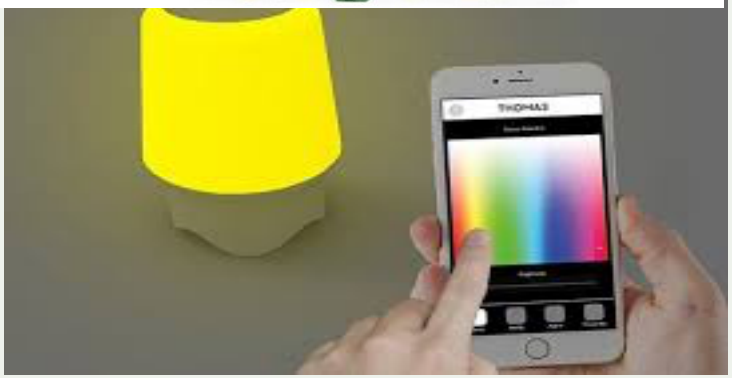
1999 – Bill Joy, Sun Microsystems
D2D Communication
– **Kevin Ashton, MIT, AutoID**
... RFID Everywhere **...**

Internet ... IoT (com I)

2000 .... 2010 ...

Coisas, Dispositivos:

Just for Fun ?



Coisas, Dispositivos:

Just for Fun ?

Muitas "coisas", mais ou menos baratas
de baixo consumo e de instalação "agilizada":

ex., *passwords* fracas,
controlo de acesso facilitado

=>

Weareables

Recursos Constrangidos
Não (ou pouco) atualizáveis (*no patching*)
De qualidade discutível ... ?
... Muito vulneráveis nas garantias de confiabilidade
(sem segurança por desenho)

Óptimas coisas para elementos de botnets e para aumento da superfície de ataque de infraestruturas críticas onde possam estar inseridos

IoT (Informalmente mas factualmente)

Uma "**poeira**" de pequenos objetos (**sensores, controladores, actuadores**), que "está **inevitavelmente e sub-repticiamente**" **a invadir o nosso quotidiano e as nossas vidas**

Objetos eventualmente acionáveis (controláveis ?) com a ajuda dos nossos telemóveis

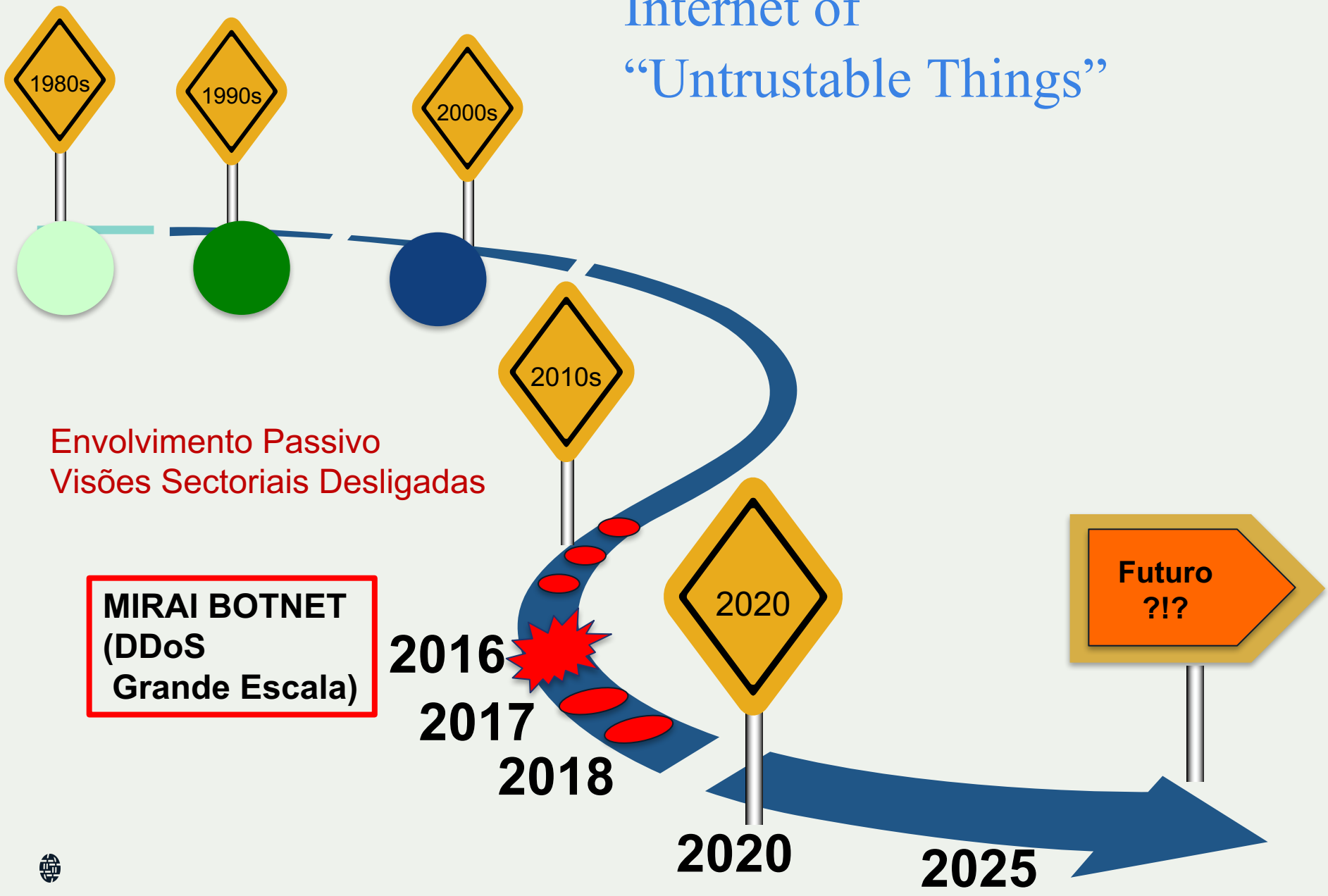
Objetos foram sendo globalmente interligados em infraestruturas computacionais, produzindo dados e decidindo ações, e são hoje facto hoje soluções consolidadas em serviços na CLOUD

> CLOUD IoT provisioning aaS

Internet ... IoT (com I)

2010 ... 2018

Internet of "Untrustable Things"



IoT e Top Ten Vulnerabilities, OWASP*

I1. Insecure Web Interface
I2. Insufficient Authentication/Authorization
I3. Insecure Network Services
I4. Lack of Transport Encryption/Integrity Verification
I5. Privacy Concerns
I6. Insecure Cloud Interface
I7. Insecure Mobile Interface
I8. Insufficient Security Configurability
I9. Insecure Software/Firmware
I10. Poor Physical Security

Envolvimento Passivo
Visões Sectoriais Desligadas

Situação recente tem revelado os perigos de uma IoT insegura e não confiável ...

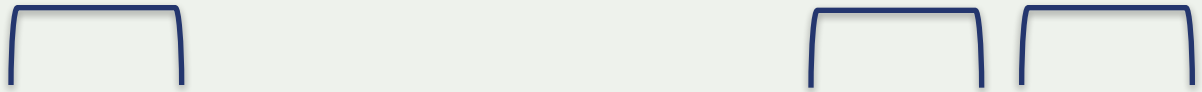
E em que a simples "auto-regulação" parace não ter funcionado ...

https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

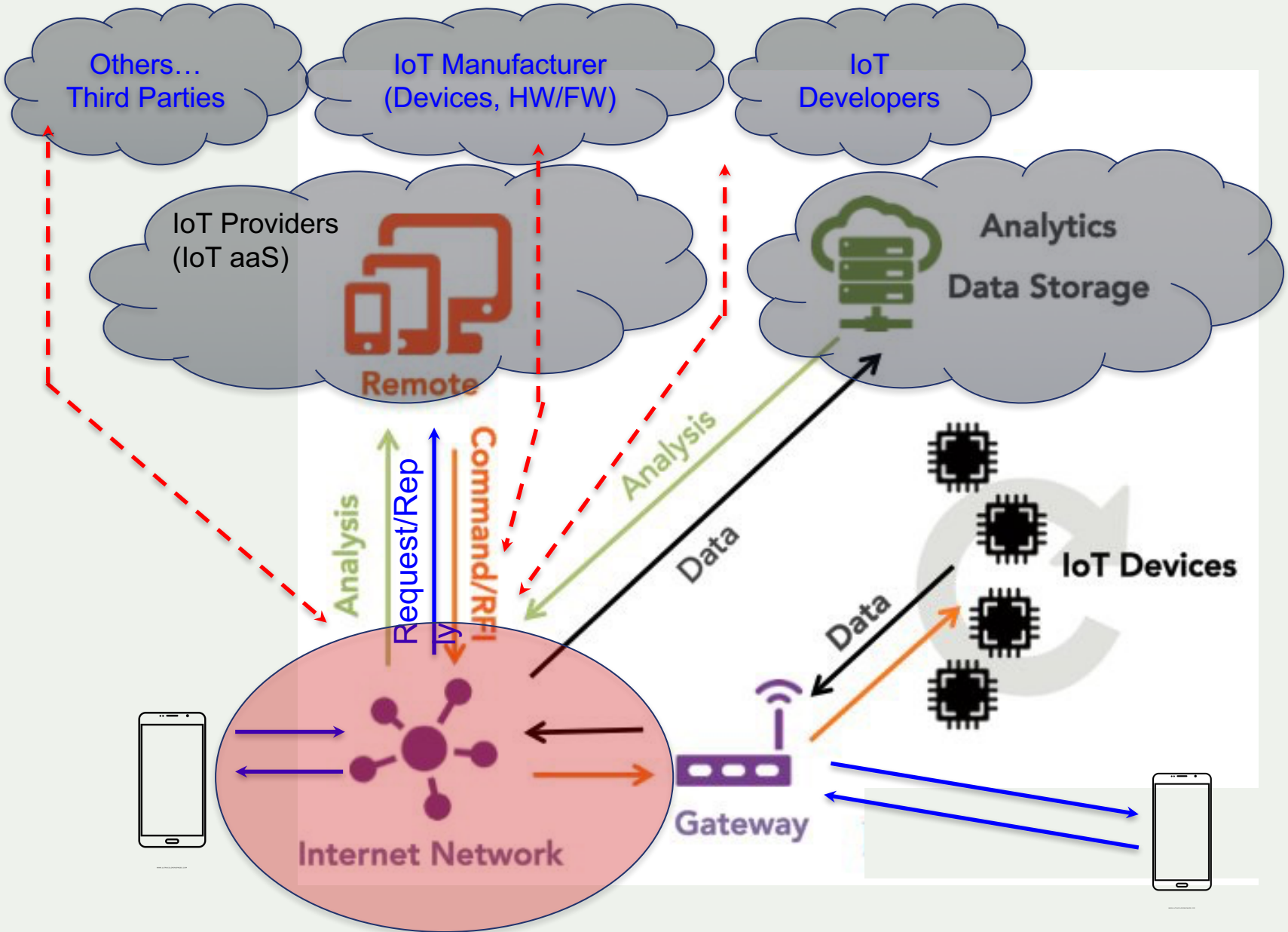
IoT ... Comunicação “sem I”

Curto alcance:
Bluetooth/Bluetooth Low Energy (BLE)
Zigbee … Zigbee 3.0, ZWave
IEEE 802.15.4
Wi-Fi/Wi-Fi HaLow50, Near Field Communication (NFC)
Radio Frequency Identification (RFID);
…
Longo alcance:
LoRaWAN, SigFox, NarrowBand-IoT (NB-IoT) LTE-M, …

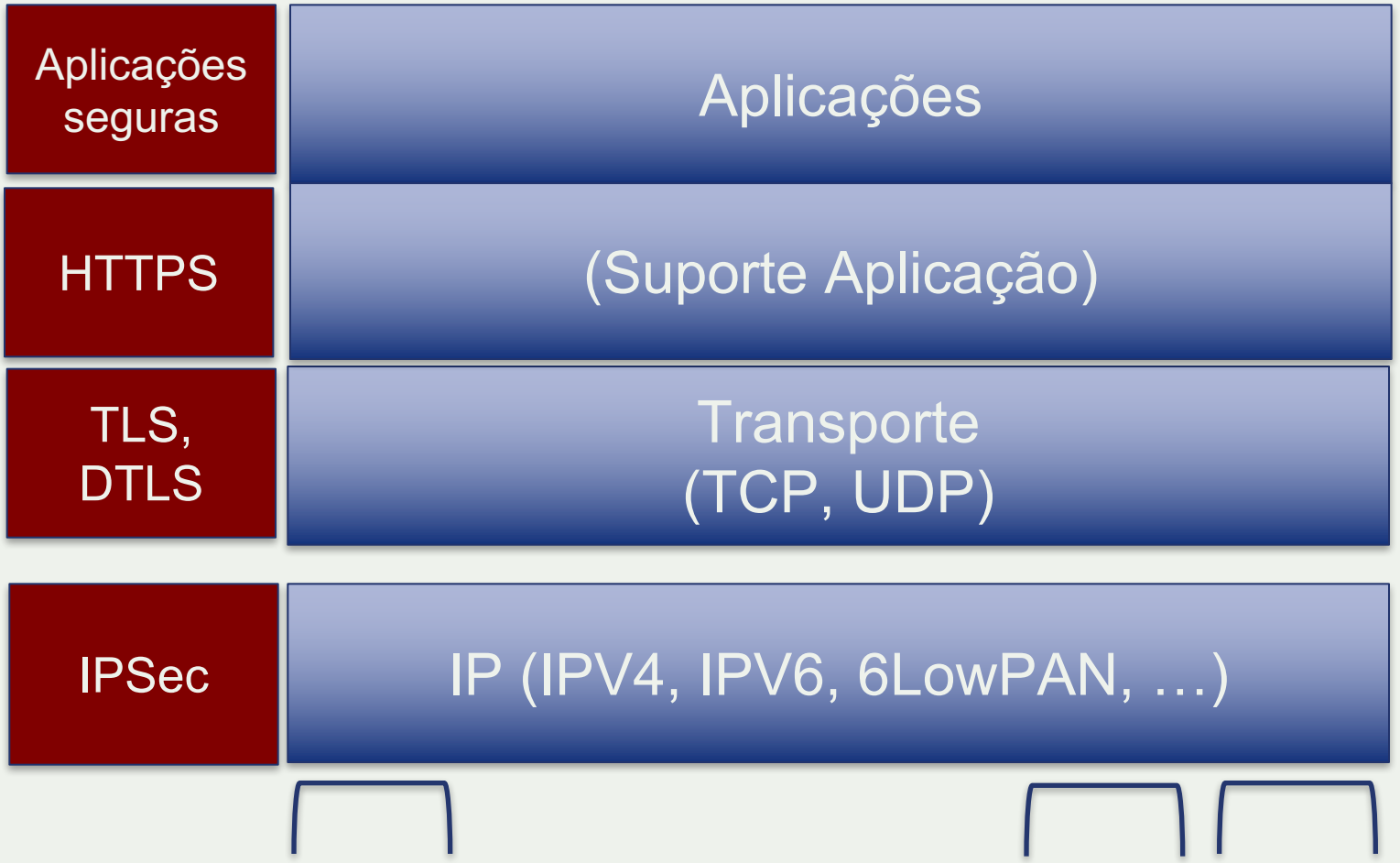
Outros:
Ethernet, USB, SPI, MIPI and I2C
Non-IP based protocols: SMS, LiDar, Radar, etc…



Cloud-Based IoT aaS / Complexidade Multi-Stack



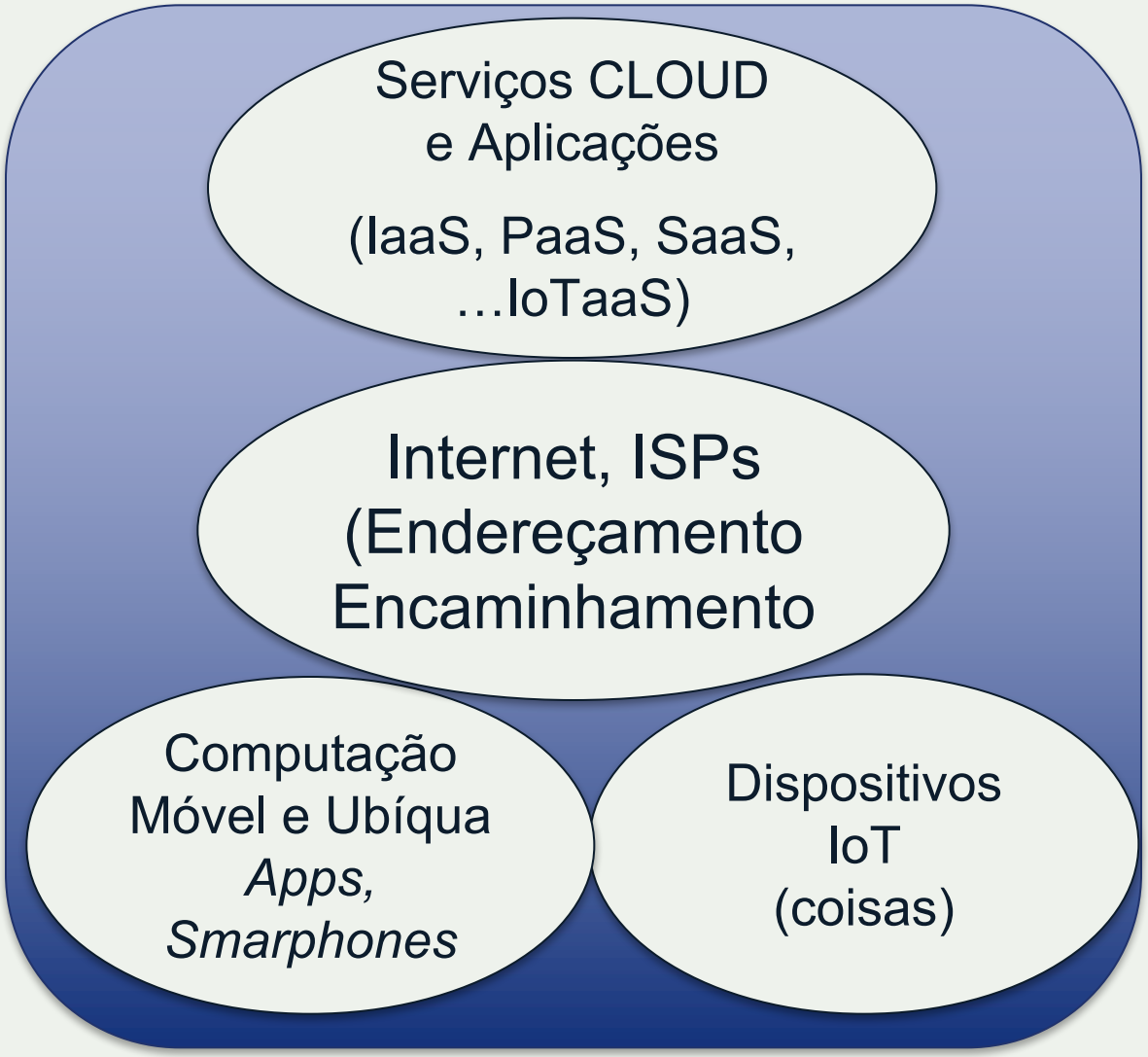
Internet of … Everithing (IoeT)



DATA-LINK / MEDIUM ACCESS PROTOCOLS

… Tudo o que for interessante suportar, de forma normalizada, aberta e interoperável

Convergências em plataformas IoT



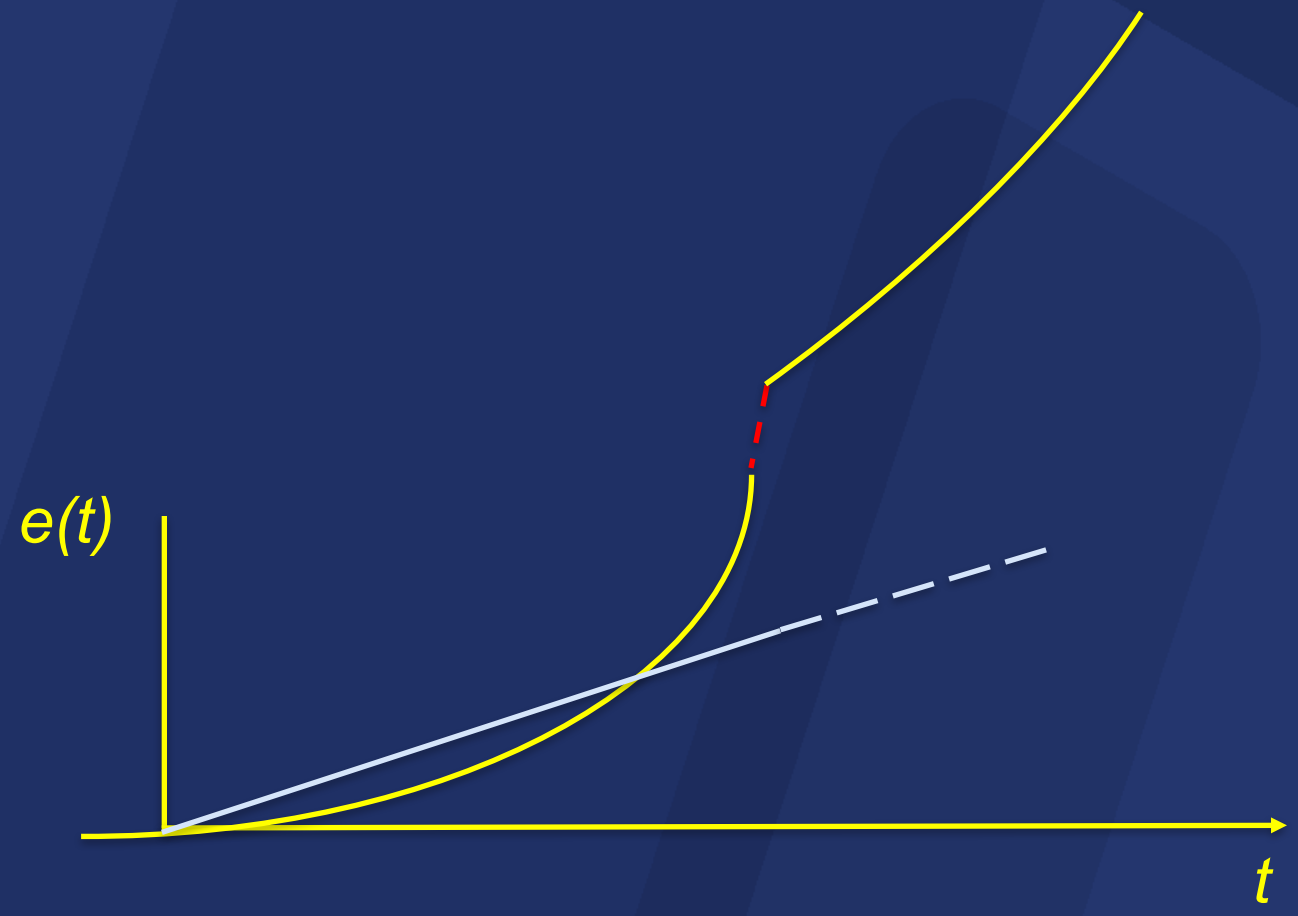
IoT ... > IoeT

2018 ...

Crescimento Sustentável ?

IoT

Expansão Futura



Explosão da IoT … IoeT … e os perigos de uma IoUT

Projeções *

Dispositivos:

6,4 Biliões em 2016/2017

20,8 Biliões em 2020 ~65% Consumo

75 a 100 Biliões em 2025

Valor do Mercado:

235 B USD$ em 2016

273 B USD$ em 2017

…

2,75 T USD$ em 2020 ~51 % Consumo

11 T USD $ em 2025

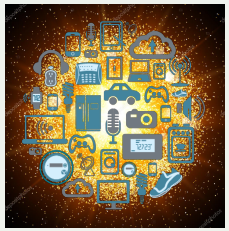
* ISOC, OTA, Gartnet Group, Statista.com

Mas como será a explosão ?

Com que modelos de interesse, de negócio, de poder ?

Explosão com Fragmentação, Bloqueamento e Entricheiramento ?
Várias IoTs em Várias Internets ? Não parece boa ideia !




...

Desintermediação e Auto-Regulação ?

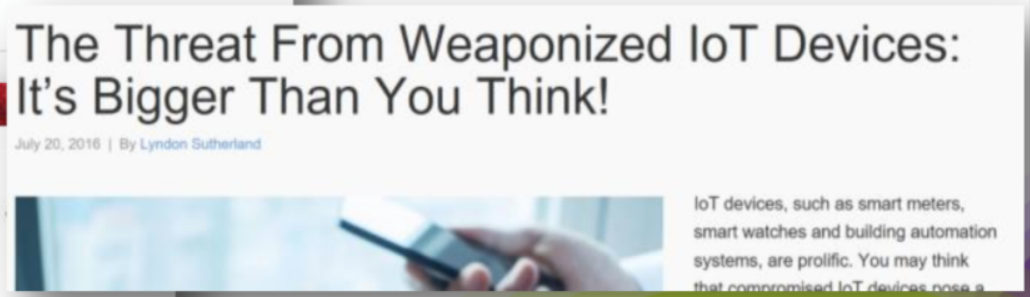
Confiabilidade
Segurança e
Privacidade

Liberdade
Independência

Utilizadores / Consumidores

A situação atual é demonstrativa
sobre o que se deve evitar no futuro !

IoUT (Internet of Untrustable Things)



IoUT (Internet of Untrustable Things)

The Romantik Seehotel Jäegerwirt 4-Star Superior Luxury Hotel was hit by a ransomware attack that locked guests in and out of the rooms.

Another singular incident involved a ransomware, the victims are hundreds of guests of a hotel in Austria, the Romantik Seehotel Jäegerwirt 4-Star Superior Hotel. The guests wer out of their rooms. The malware infected the systems at the hotel and its administration c the ransom to restore a normal operation.

Sundance Hack Acts as a Warning to Small and Mid Sized Businesses

Amanda McGuinness – January 26, 2017

36 SHARES Interesting 1 Not Interesting

017 Sundance Film Festival was underway with its first weekend of a cyberattack that disabled its online box office as well as internet attack is BI as a denial or customer tion to the s were ot cash only,

PCWorld FROM IDG

SUBSCRIBE

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | SMARTPHONES | HARDWARE | SECURITY | SOFTWARE | GADGETS

Privacy | Encryption | Antivirus

Home / Security

NEWS

The next wave of cybercrime will come through your smart TV

Always on and vulnerable, smart TVs are waiting to be attacked.

By Jeremy Kirk

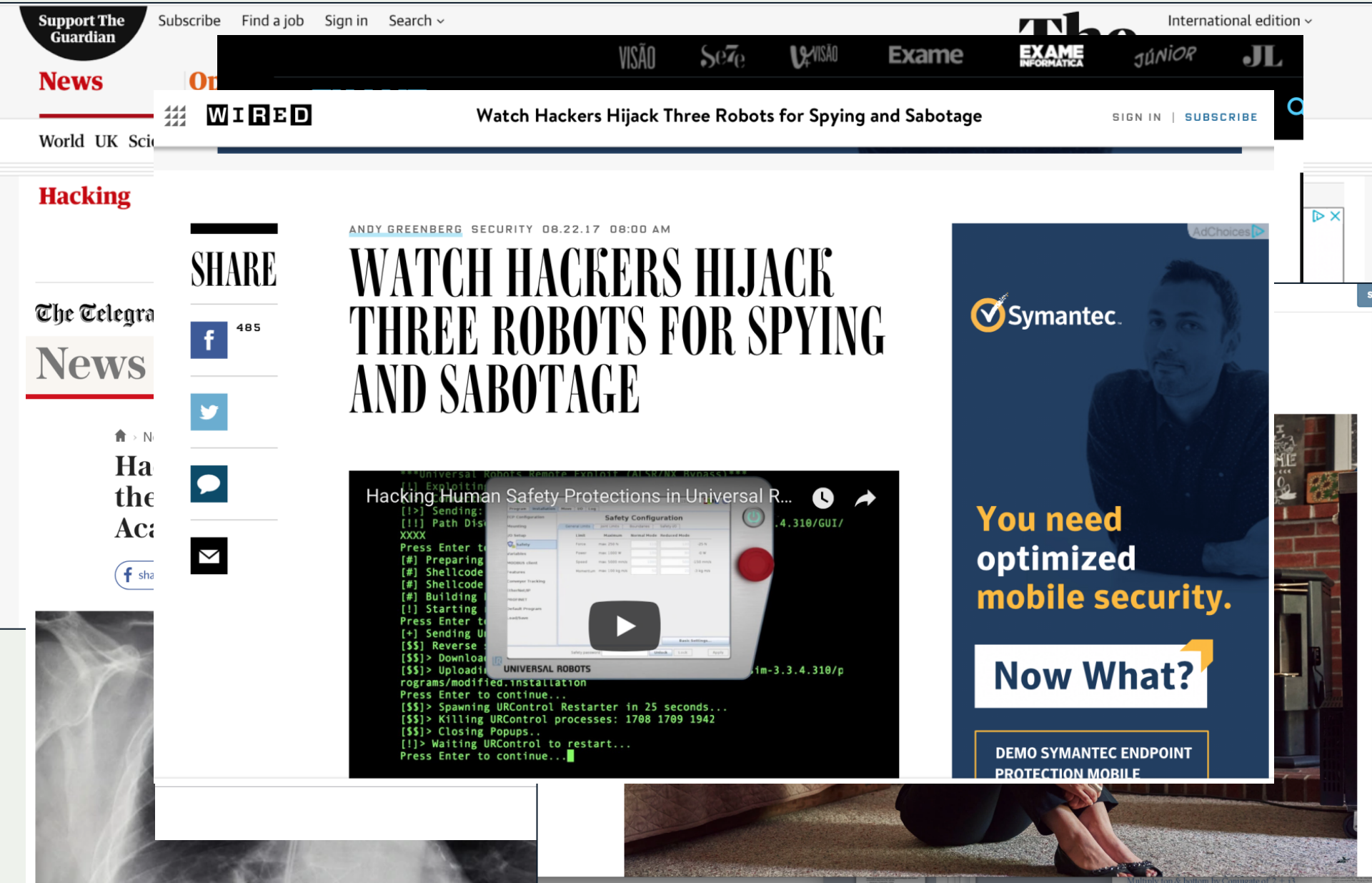
Australia Correspondent, IDG News Service | DEC 28, 2015 6:00 AM PT

Smart TVs are opening a new window of attack for cybercriminals, as the security defenses of the devices often lag far behind those of smartphones and desktop computers.

Running mobile operating systems such as Android, smart TVs present a

MORE LI

IoUT (Internet of Untrustable Things)



A Auto-Regulação … não tem funcionado !

FTC Suit Against D-Link Warns All IoT Device Makers to Boost Security

By Wayne Rash | Posted 2017-01-06 Print

Tweet LinkedIn 81 Like 26 Share 3

NEWS ANA
security, th
hard-codec
unprotecte

LAS VEGA
starting w
attorney B
and Identit

Rossen op

OTA
Online Trust Alliance

TALKING TECH BUZZ VIDEO PODCASTS

FTC: Vizio smart TVs spied on what viewers watched

Mike Snider , USA TODAY Published 3:09 p.m. ET Feb. 6, 2017 | Updated 8:42 a.m. ET Feb. 7, 2017

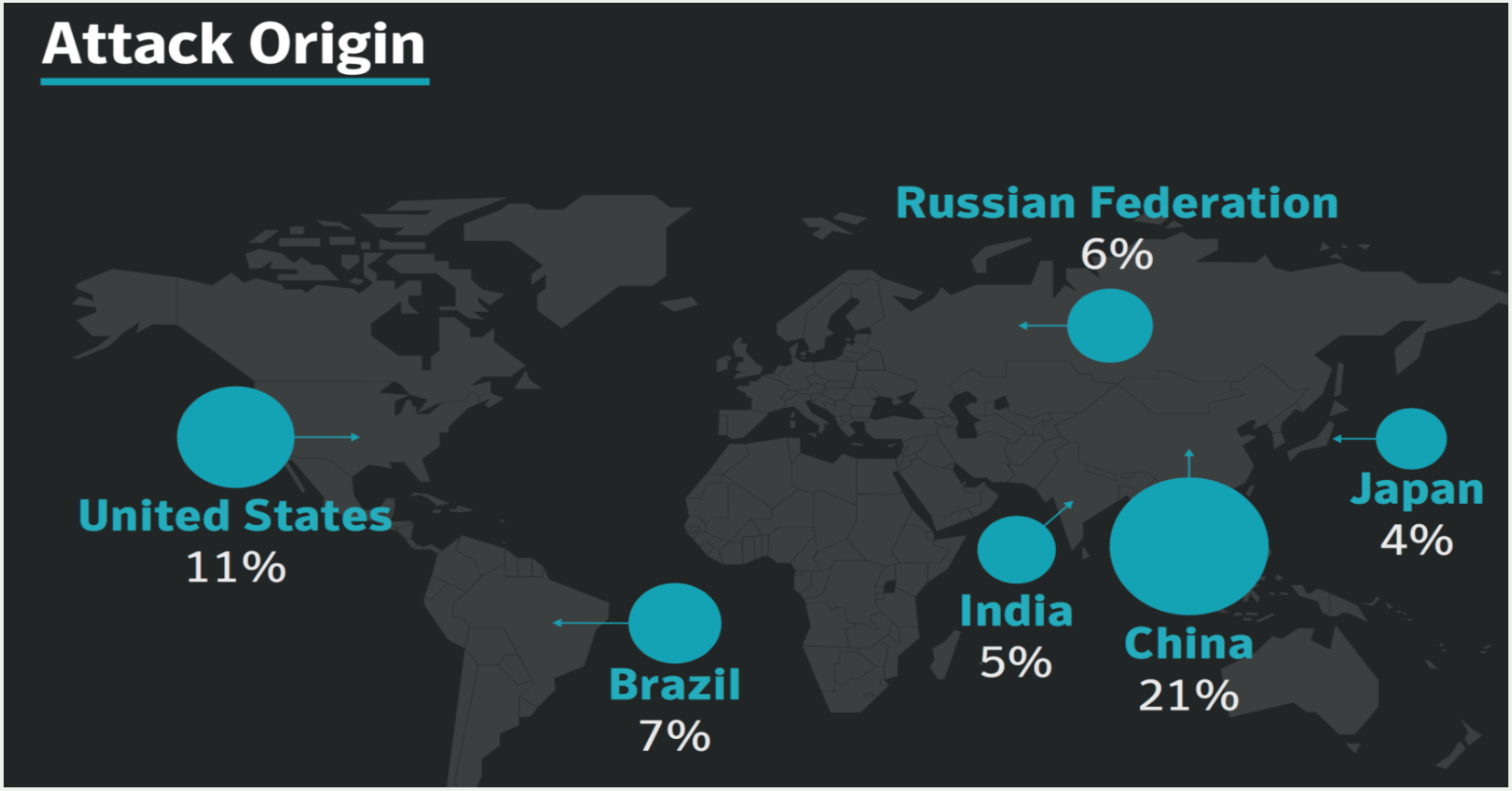
934 Shares

Vizio admits they secretly used software to track people's TV viewing habits. Now they've agree to

IoT Attacks, 2016-2017-…

https://www.symantec.com/security-center/threat-report

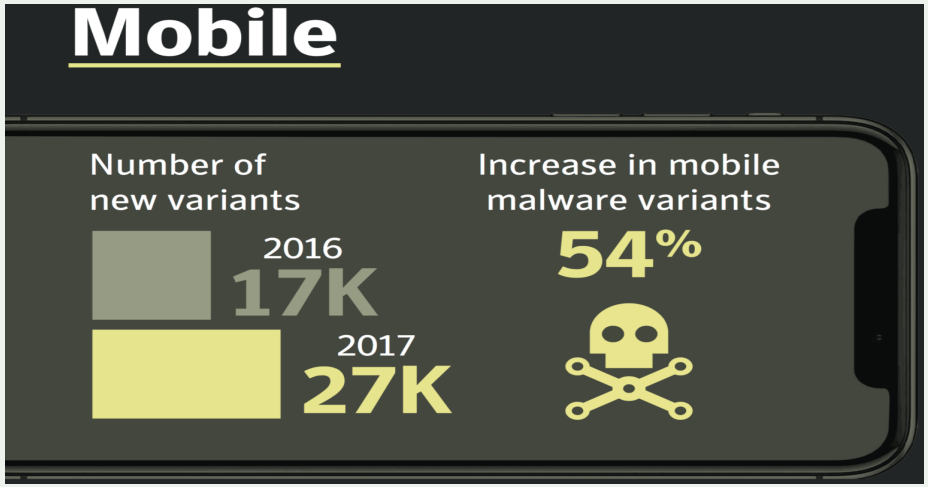
Incremento de 600% em ataques e incidentes de segurança contar diferentes tipos de dispositivos IoT

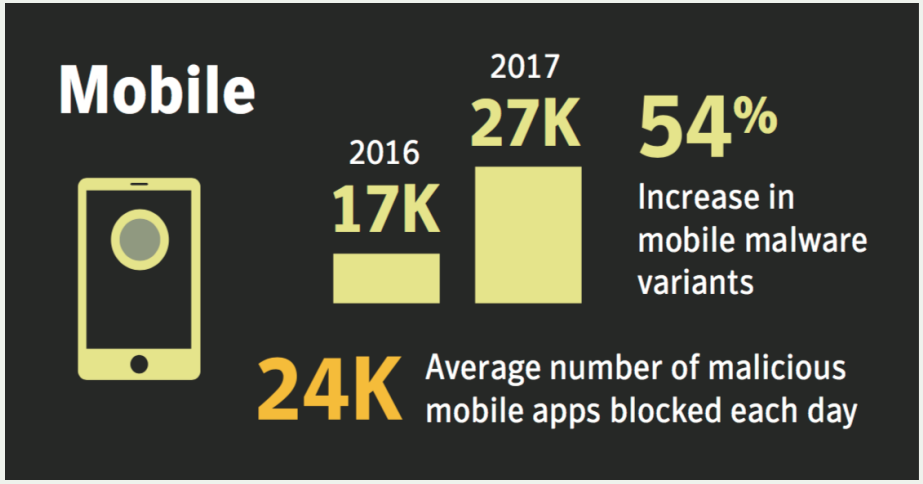


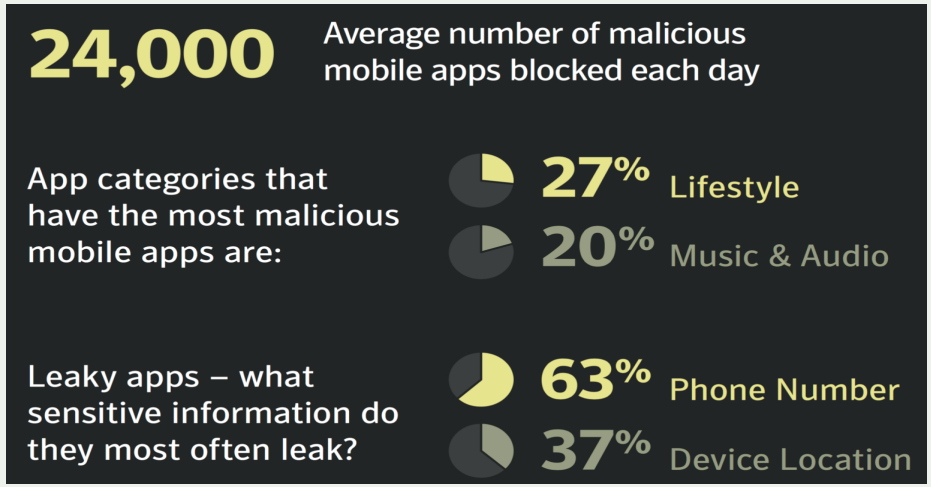
Panorama expectável de ataques na IoT (2018)

- Ataques à IoT estão a diversificar-se
- Atacantes vão explorar mais tipos de dispositivos como elementos de botnets que podem ser cada vez mais perigosas
- Os ataques envolverão *Routers*, *Modems*, *Smart Gateways/Hubs*, "*Malware" / Unsecure Apps*
- ... Uso de diferentes tipos de dispositivos infetados (combinados como fatores de amplificação de superfícies de ataque e vulnerabilidades)

Exemplos de fatores de amplificação
IoT x Mobile Apps + "BYOD" Paradigm







Symantec Security Threat Report, 2018

… A Venda de Pistolas para Hacking IoT !

Não, não é preciso comprar em Bitcoins na Dark/Deep WEB ☺

Compram-se na Internet e recebem-se pelo correio …

20 – 100 – 1000 – 3000 USD$

https://www.attify-store.com/collections/frontpage

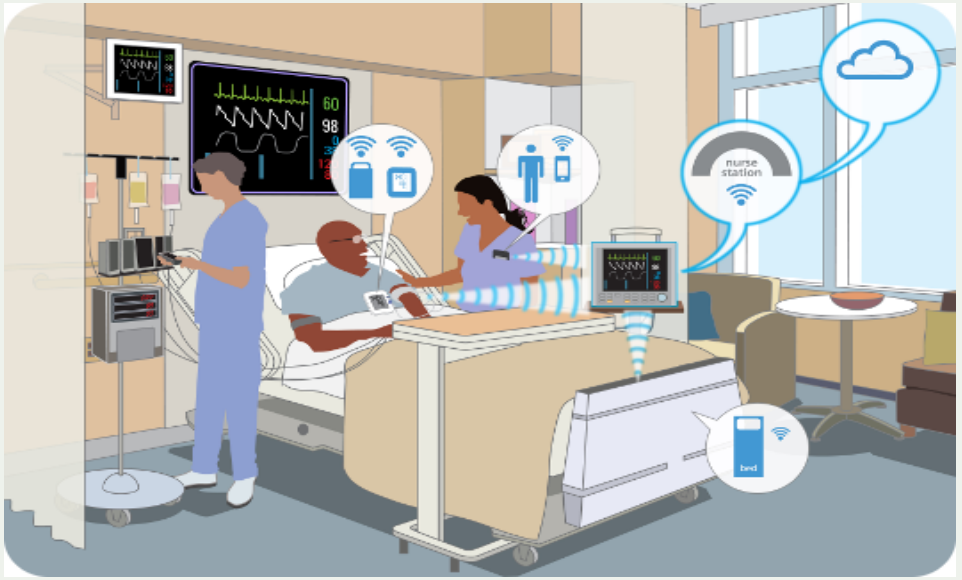
https://blog.securityevaluators.com/the-introductory-iot-hardware-hacking-tool-box-389c4605329f

Etc, etc, etc…

Crescimento da IoT em Sectores Críticos

Preocupações:
Todas as coisas ! todos os mercados ?
Mercados cada vez mais críticos !

Coisas, Dispositivos (*Not cheap, not for fun*)



Coisas, Dispositivos (*Not cheap, not for fun*)

Alargamento e Consolidação da IoT em Diferentes Setores (Aplicações, Serviço e Mercados Verticais)

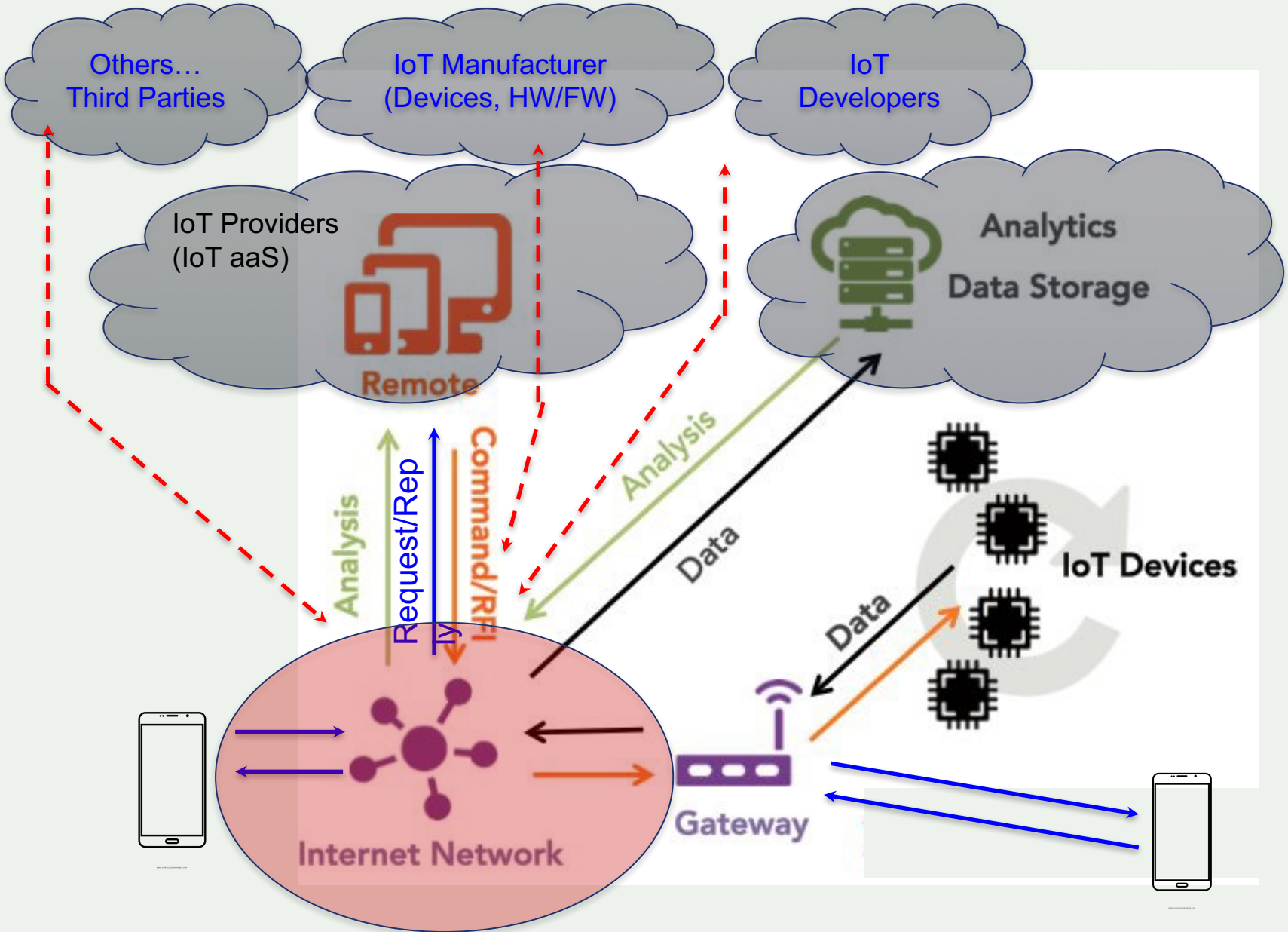
- *Smart Homes*
- *Smart Cities*
- *Intelligent Public Transport*
- *Smart Grids*
- *Smart Cars*
- *Smart Airports*
- *eHealth & Smart Hospitals / Medical Care Change Driving Factors*
- *Smart Supply-Chaining*
- *Smart Water-Management*

Urgente: passar de um envolvimento passivo para um envolvimento ativo, com policy-makers mais ativos num modelo de responsabilidades multi-stakeholder

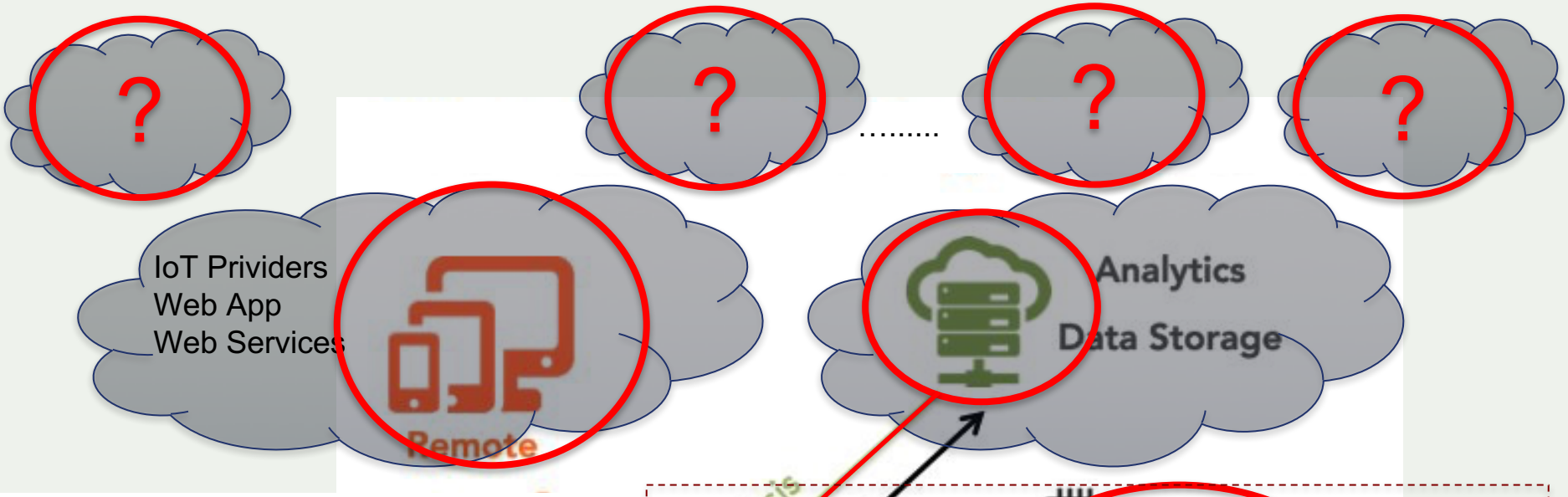
Convergência para modelos e arquiteturas
IoT como soluções confiáveis,
com segurança e privacidade

Complexidades, Dificuldades e Desafios

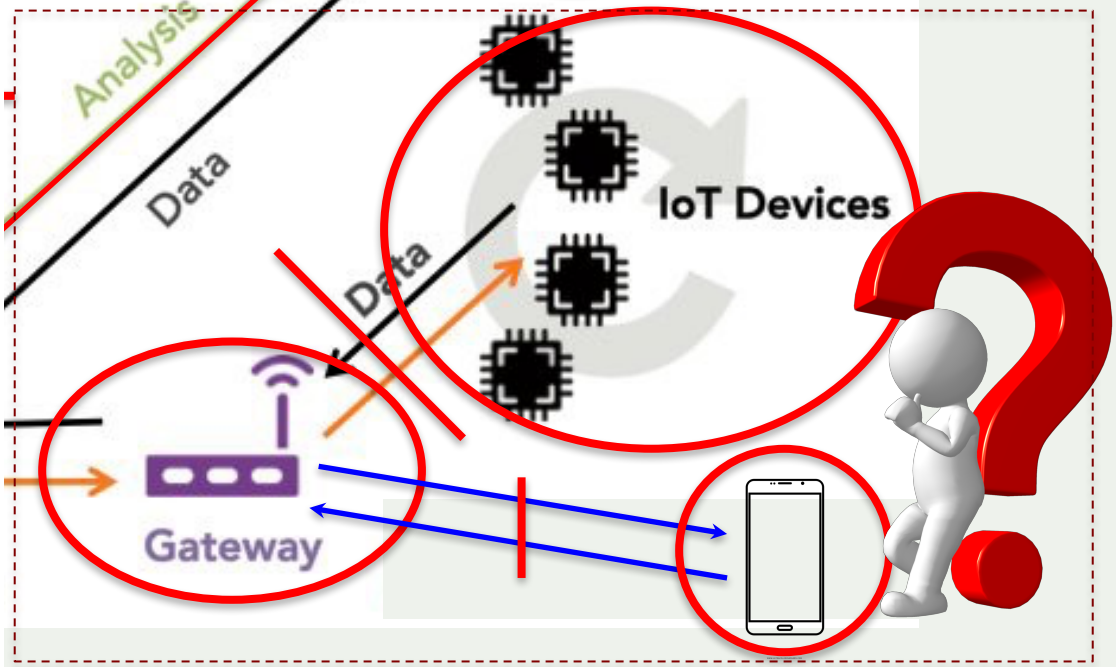
Existe um modelo arquitetural comum ?



Aumento da superfície de ataques na IoT ?



Fabricantes:
(*"Black Box" Devices ?*)
Desenvolvedores:
(*Quality Assurance ?*)
Regulação
(*Ethics, Law, Compliance and Guidance?*)
Economia IoT:
Modelo de Incentivo e responsabilidades ?



Desafios da Confiabilidade, Segurança e Privacidade
Pode Abordar-se uma Base Comum de Segurança ?

Muitos ambientes de comunicações (dispositivo-dispositivo, dispositivo-smart hubs)

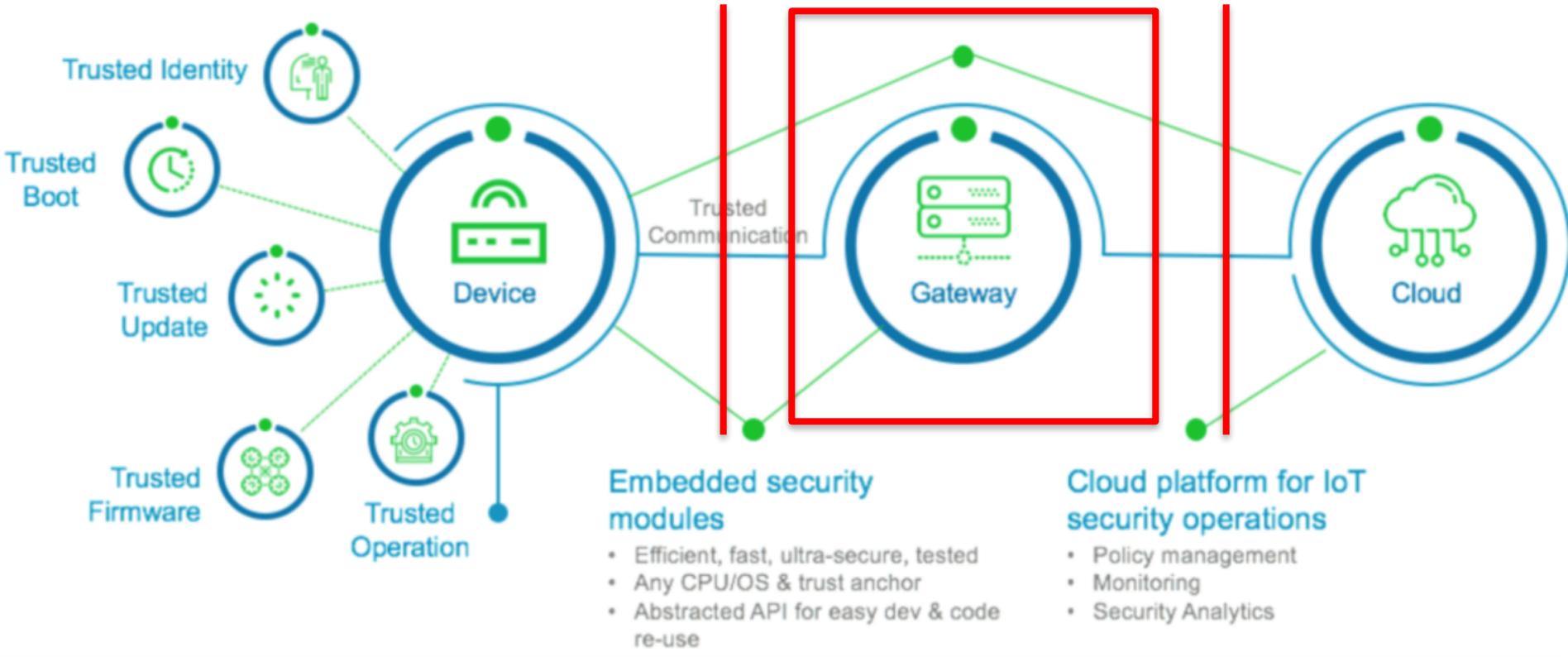
Curto alcance:
Bluetooth/Bluetooth Low Energy (BLE)
Zigbee … Zigbee 3.0, ZWave
IEEE 802.15.4
Wi-Fi/Wi-Fi HaLow50, Near Field Communication (NFC)
Radio Frequency Identification (RFID);

Longo alcance:
LoRaWAN, SigFox, NarrowBand-IoT (NB-IoT) LTE-M.

Outros:
Ethernet, USB, SPI, MIPI and I2C
Non-IP based protocols: SMS, LiDar, Radar, etc.

(*) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

O Papel de "Smart Hubs / Gateways"



Funções dos
Smart Gateways ou
Smart Hubs

Elementos Críticos
Elementos Chave !

Tipologia de Ameaças e definição de novos modelos de Adversário para Segurança por Desenho

ENISA, Nov 2017

Baseline Security Recommendations for IoT *

Framework com visão abrangente de todos os elementos da IoT:

- Coisas (Dispositivos)
- Sensores e Actuadores
- Sistemas Embebidos

- Comunicações: uma enorme plêiade de protocolos de comunicação sem fios

- Suporte de decisão inteligente

(*) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Mas o estabelecimento de modelos de referência comuns para interoperabilidade, confiabilidade, segurança e privacidade é um problema complexo e difícil de abordar ...

Desafios da Confiabilidade, Segurança e Privacidade
Pode Abordar-se uma Base Comum de Segurança

Muitas iniciativas de modelos e *frameworks* de normalização de arquiteturas... Como harmonizar ?

AIOTI High Level Architecture functional model62

FP7-ICT – IoT-A Architectural reference model63

NIST Network of Things (NoT)

ITU-T IoT reference model

ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)

ISACA Conceptual IoT Architecture

oneM2M Architecture Model

IEEE P2413 - Standard for an Architectural Framework

…

Desafios da Confiabilidade, Segurança e Privacidade
Pode Abordar-se uma Base Comum de Segurança

Muitas Plataformas .... Não Interoperáveis !!!

Plataformas CLOUD, Edge-Based + Fog-Integration (Exemplos, 2018):

Google ITTT – If This then That
Google Cloud IoT
MS Azure IoT Suite
SAP Cloud Platform for IoT
Salesforce IoT
Oracle IoT
Cisco IoT Cloud Connect
Bosh IoT Suite
IBM Watson IoT
ThingWorx IoT Platform

OpenSource:

Fiware Platform for Smart Digital Future
ThingsBoard, Kinoma, Arm MBED, Snappy Core Platform, Node Red
Iotivity, DSA

IAB – IETF – IoT *Directorate*

(https://www.ietf.org/topics/iot/)

Esforço e Agenda para a Interoperabilidade
(num movimento efetivo *muti-stakeholder* ...)

Agenda IETF

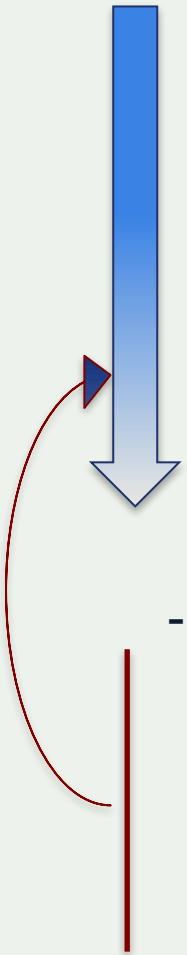
https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/

Uma pilha de referência para interoperabilidade

Nível Sessão		AMQP, CoAP, DDS, MQTT, XMPP
Nível REDE	Encapsulamento	6LowPAN, Thread
	Encaminhamento	CARP, RPL
Segurança Nível Data-LINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

(*) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IoT Security Enforcement Standards: DEVICE-LEVEL



ZWave S2 (rfc7428) …. POWELINE Security, DECT ULE

BLE (rfc 7668) + BLE Security, IEEE 8015.4 WPAN

IEEE 802.11i WLAN Security

- **+ Network Access Control: EAP and 802.1X**

6LowPan / 6LowPan Security, 6LowPan e Data-Link Mappings

ROLL: CARP / RPL (rfc 6550)

DTLS Enabled Transport

- - - - - -

(Provable) Secure Light-Weight Pairing of Cryptographic Keys and Establishment of Security Association Parameters

Randomization + Key Generation + Rekeying Protocols

Criptografia ECC

Protocolos nível sessão

New IETF IoT Standards for IoT Interoperability

2016

ACE rfc7744 and … (Authorization and Authentication in Constrained Environments): OAuth 2.0 based profile for IoT

CoAP rfc7252 (Constrained Application Protocol)

CBOR rfc8392 (Concise Binary Object Representation)

2017

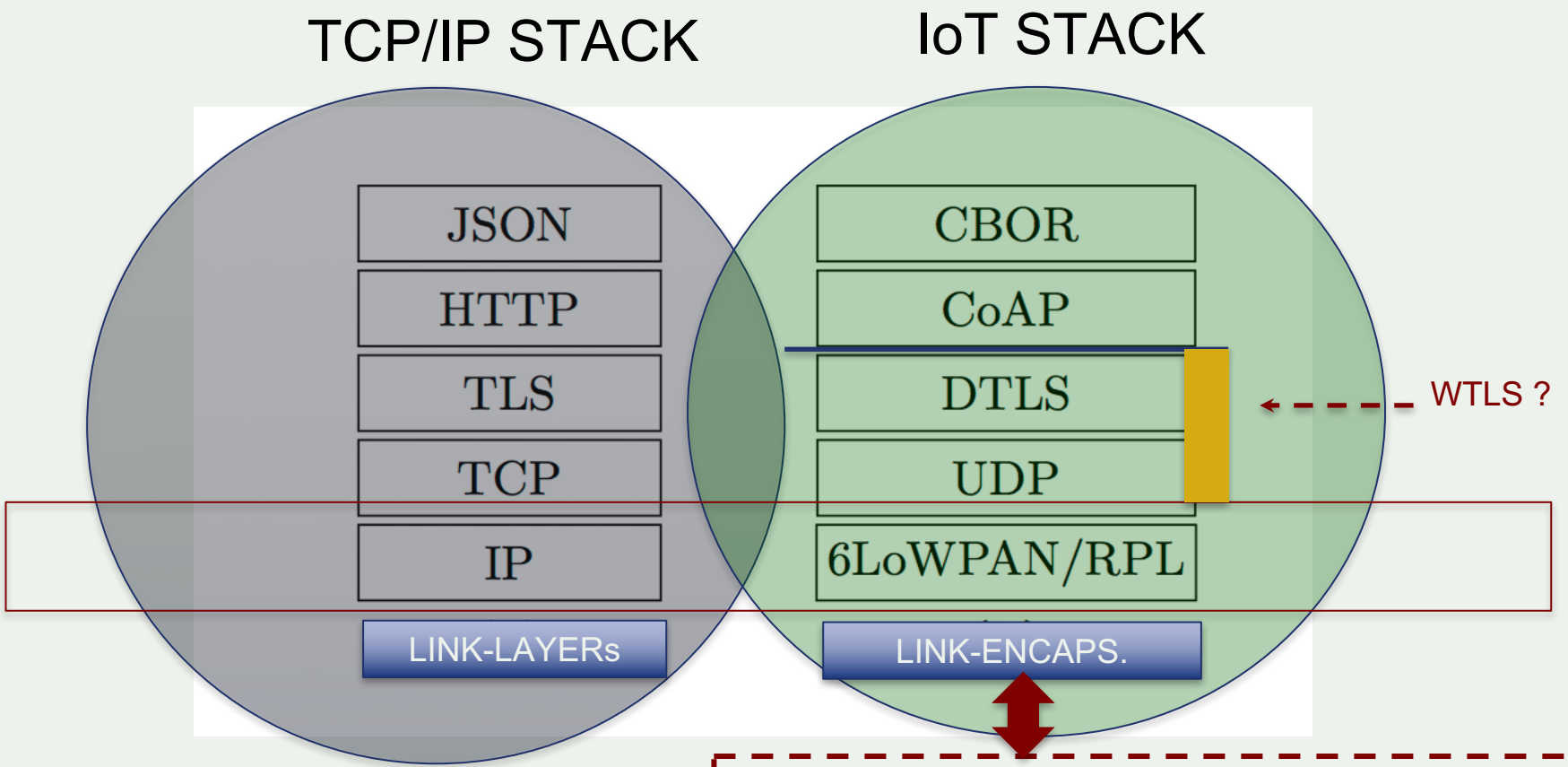
CoRE rfc6690 (Constrained Restful Environments)

COSE rfc 8152 … (CBOR Object Signing & Encryption for CBOR Protection)

2018

OSCoAP Draft RFC (Object Security for CoAP)

IETF IoT Standards: Roadmap for Secure Interoperablity w/ Constrained Devices



Conclusões, Linhas de Ação *e Recomendações ...*

Precisamos de atuar para uma IoT Confiável e Sustentável

Identificação de *GAPs*

- Fragmentação da regulação e das abordagens de segurança
- Falta de Informação e Conhecimento (+ *Awareness*) e Consumidores como o "Elo Mais Fraco" !
- Falta de informação clara sobre o ciclo de vida de produtos
- Dispositivos inseguros e sem atualizações face a vulnerabilidades (*no patching*) com FW e desenvolvimento de SW inseguros
  - Atualização de "firmware" e "software" com enormes desafios): "*Over the Air Updates*"
- Falta de interoperabilidade entre dispositivos, plataformas, *frameworks* e arquiteturas
- Falta de incentivos económicos para estabelecimento de uma economia de confiança nos mercados da IoT

Responder aos desafios e problemas atuais (1)

- Uma enorme superfície de ameaças e de potencial ataque
- Proliferação de dispositivos de baixo custo, com recursos limitados e com limitações graves de segurança
- Dispositivos (*smart things*) podem ser os novos "*smart cookies*" que atentam contra a privacidade dos seus utilizadores ou consumidores
- A IoT como ecossistema de grande complexidade
- Desenvolvimento e operacionalização em grande escala e a um ritmo sem precedentes

Responder aos desafios e problemas atuais (2)

- Há o perigo da expansão da IoT com Fragmentação e Entrincheiramento das Soluções
- Divergências de fornecedores e provedores de serviços quanto à integração de mecanismos de segurança e quanto ao controlo dos utilizadores e consumidores
  - Quais os incentivos ?
- Falta de *expertise* com visão “full stack” face ao Ecossistema atual ao nível dos desenvolvedores, integradores e promotores de serviços IoT
- Segurança e Privacidade (por concepção): Requerem a Definição rigorosa e adequada de novos Modelos de Adversário

Responder aos Desafios (3)

- Fatores difíceis de conciliar: *Time To Market*, Pressão Comercial, Competição pelo Baixo Custo (impossível de acomodar com "Segurança e Privacidade por Desenho"
- Evitar modelos de negócio vs. modelos de responsabilidades "obscuros" (com responsabilidade face aos utilizadores e consumidores)

Compreender e Definir os novos Modelos de Adversário

Risco = Vulnerabilidades x Potencial da Ameaça

Risco (t) = Vulnerabilidades (t) x Potencial de Ameaça (t)

Vulnerabilidades "intrínsecas":

- Ausência de mecanismos de confiabilidade "por concepção" (*Dependability by Design*)

  Dependability =
  Reliability + *Safety* + *Security* + *Privacy*

- **Segurança e Privacidade: Requerem a Definição Rigorosa de Novos Modelos de Adversário para promover soluções de Segurança e Privacidade "por desenho"**

Desafios Relevantes para uma IoT sustentável:

- *IoT Trust Framework (v2.5, Oct/2017): The 40 Principles and Requirements: Must, Should (Reuired, Recommended)*

- *Security Principles: Dispositivos. Apps e Serviços Cloud (12)*
- *Access Control Management (5)*
- *Privacy, Disclusures nd Transparency (16)*
- *Notificatons & Related Best Practices (7)*

https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Desafios Urgentes (*Multi-Stakeholders*):

Segurança

Mais robustez e serviços de segurança com gestão transparente dos ciclos de vida de dispositivos, produtos e serviços IoT

Interoperabilidade e Normalização

Uso voluntáirio de normas abertas, amplamente e consensualmente escrutinadas, disponibilizadas como "building blocks" técnicos.

Privacidade

Promoção de transparência, justiça/responsabilidade e respeito pela independência dos utilizadores/consumidores sobre as opções tecnológicas disponíveis

Aspetos Éticos, Legais e Regulatórios

Adequação e respostas em Tempo oportuno. Engajamento ativo dos decisores políticos !

Promoção de uma Economia de Confiança na IoT:

Modelo de Incentivos, Certificação de Qualidade, Defesa do Consumidor

Uma agenda urgente: utilizadores e consumidores mais atentos - como promover?

Sugestões para a agenda (Utilizadores)

Curto-Prazo (já)

Inventariar os dispositivos – "boardroom to breakroom"

Utilização de CheckLists disponíveis

(ver em: https://otalliance.org/resources/iot-resources):

- **Enterprise IoT Security Checklist - released April 17, 2018**
- **Smart Home Checklist, Advice for Buyers, Sellers & Renters - updated March 2017**

Médio-Prazo (~3 meses):

Completar auditorias de segurança de dispositivos utilizados e obter informação sobre vulnerabilidades identificadas

Exigir Patching aos respetivos fornecedores

Revogar o acesso a dispositivos vulneráveis ou "orfãos" de atualizações

Médio-Longo Prazo:

- Estabelecer um processo de gestão de atualizações
- Obter informação de conformidade sobre o ciclo de vida dos produtos e serviços

Recursos

Online Trust Alliance: otalliance.org/IoT
Internet Society: www.internetsociety.org/IoT

IoT Security & Privacy Trust Framework v2.5
https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Enterprise IoT Security Checklist
https://otalliance.org/system/files/files/initiative/documents/enterprise_iot_checklist.pdf

Smart Home Checklist
https://otalliance.org/system/files/files/initiative/documents/smart_home_check_list_3-17.pdf

Agenda para a normalização e interoperabilidade no IETF (2018):
https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/

ENISA: Baseline Security Recommendations in the Context of Critical Infrastructures
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Obrigado