Segurança na IoT

Perspectiva geral e o caso SmartThings

Seminário

2019

Nuno Santos

TÉCNICO LISBOA

O que é a Internet of Things (IoT)?

- O último grito na evolução da Internet: comunicações *machine-to-machine* (ou *device-to-device*)

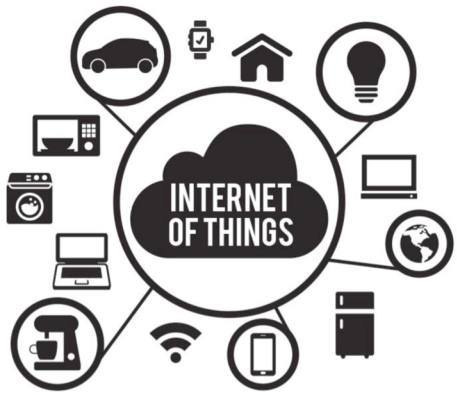
Contents (WWW)

⬇

Services (WEB 2.0)

⬇

People (Social Media)



Definição de IoT

- "Network of physical objects, devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data."

Wikipedia

- "Network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."

Gartner

Mais definições

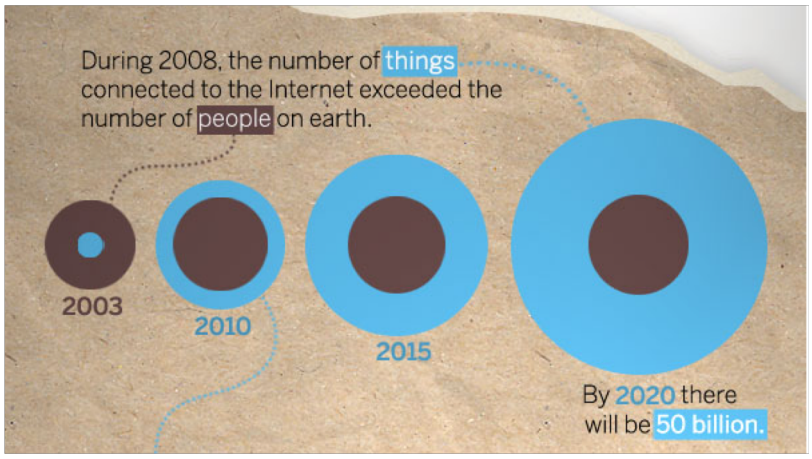
- "It is a global network of interconnected objects, **uniquely identifiable** based on a **standard** communication protocol."

[CERP-IoT 2010]

- "The Internet of Things allows people and things to be connected **Anytime, Anyplace,** with **Anything** and **Anyone**, ideally using Any path/network and Any service."

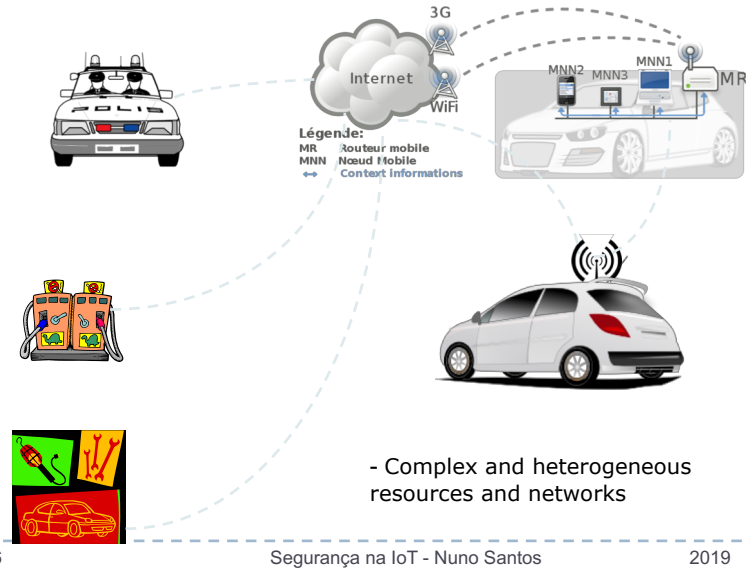
[Perera et al. 2014]

“Coisas” ligadas à Internet



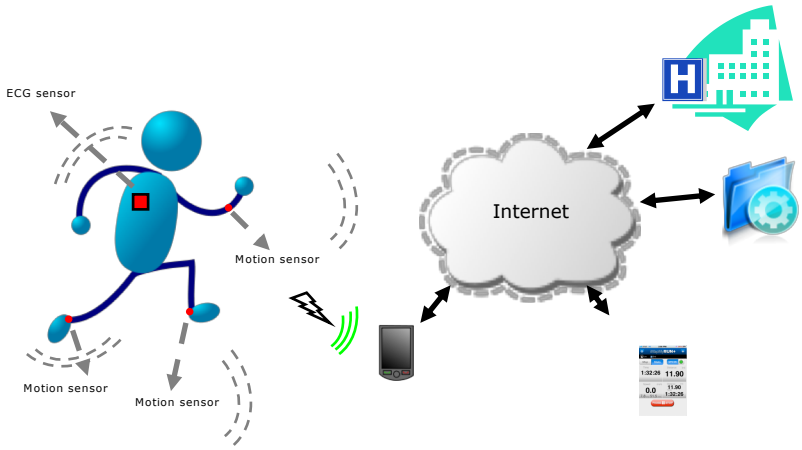
Sources: Cisco IBSG, Jim Cicconi, AT&T , Steve Leibson, Computer History Museum, CNN, University of Michigan, Fraunhofer

“Coisas” ligadas a “coisas”



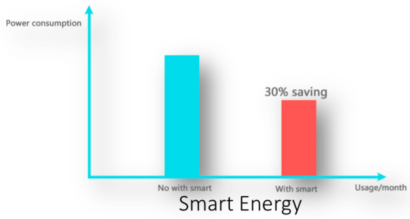
- Complex and heterogeneous resources and networks

Pessoas ligadas a “coisas”



“IoT enables de future”

Smart Homes



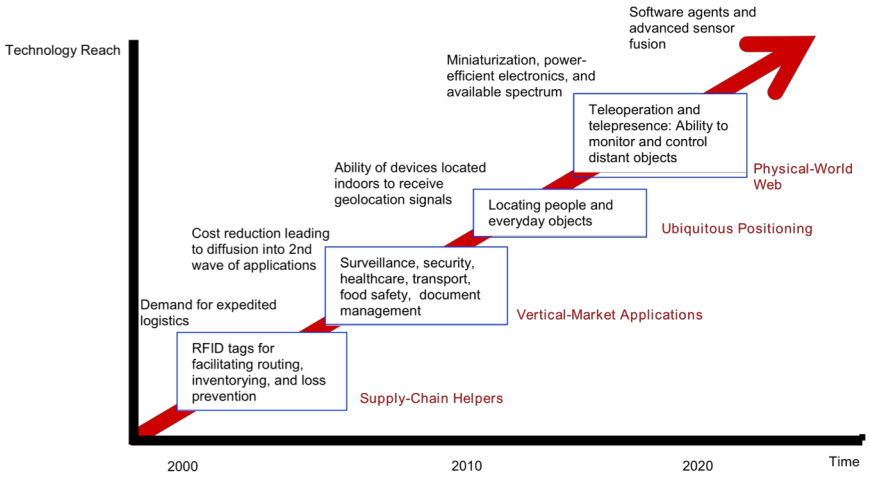
Smart Energy

Healthcare

Smart Farms

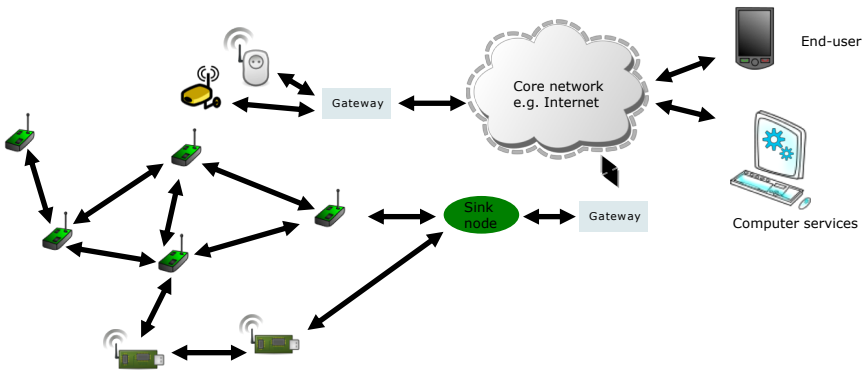
Tendências da tecnologia

TECHNOLOGY ROADMAP: THE INTERNET OF THINGS



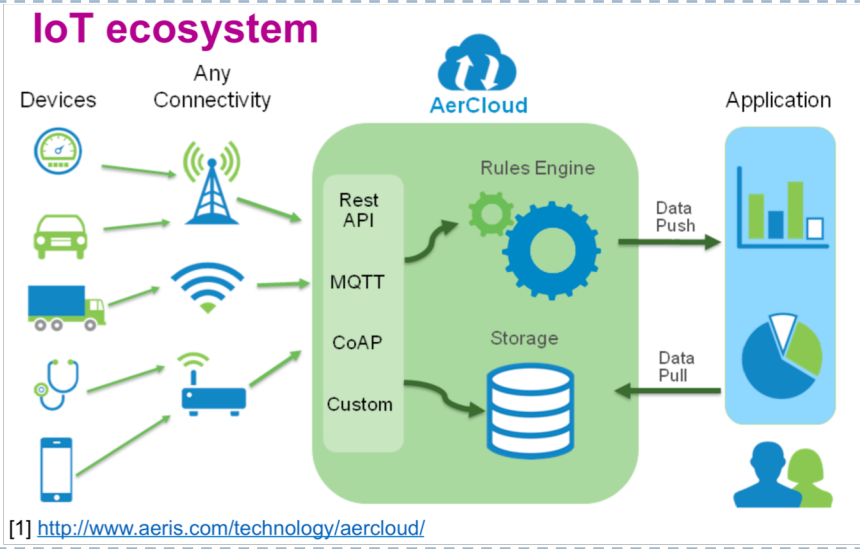
Source: SRI Consulting Business Intelligence

Proliferação de redes wireless de sensores



As redes tipicamente envolvem dispositivos de baixo consumo
Consistem em um ou mais sensores, podem ser de diferentes tipos (ou actuadores)

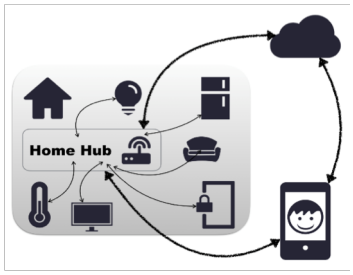
Ecosistema IoT oferecido por provedor de serviço



[1] http://www.aeris.com/technology/aercloud/

SmartHome: Casa inteligente

- Plataformas para SmartHome usam **home hubs** para interligar *smart devices* de diferentes fabricantes




Amazon Echo


Google Home


Apple HomeKit


Samsung SmartThings

Duas faces da segurança: *safety* e *segurança*

> Safety: The expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.
> ISO/IEC/IEEE 24765:2010 "Systems and software engineering — Vocabulary"

Difference	Safety	Security
Difference in entities to protect	People's lives, properties (houses, etc.), etc.	Confidentiality, integrity, availability of information, etc.
Difference in causes	Reasonably foreseeable misuse, malfunction of devices	Intended attacks
Difference in damage detection	Easily detected since damage appears as accidents	Most incidents are difficult to detect; for instance, tapping, intrusion, etc.
Frequency of occurrence	Can be addressed as the probability of occurrence	Hard to be addressed in terms of the probability because attacks are made intentionally by humans
Timing of taking measures	Dealt with by risk analysis/treatment at the design phase	Since new attack methods are developed as time passes, continued analysis/treatment is necessary

Problemas de *safety*: Exemplos de acidentes

Period of media coverage	Device involved	Description
2005	Stock ordering system	Transactions of erroneous orders of 42 times the number of stocks issued were closed and could not be canceled due to a software defect.
2006	Self-balancing electric bicycle	Due to a software defect, tires may rotate backwards, placing drivers at the risk of being thrown off.
2008	Monorail	Due to high-frequency noise in the power-supply unit, an inverter failed to recognize operations, resulting in abnormal acceleration that caused the train to overrun. Because it was a single-track railway, there was also a possibility of a crash.
2014	Large truck	A defect in the control program of the gearbox disabled the detection of the gear select position, posing a risk of wrong gear change.

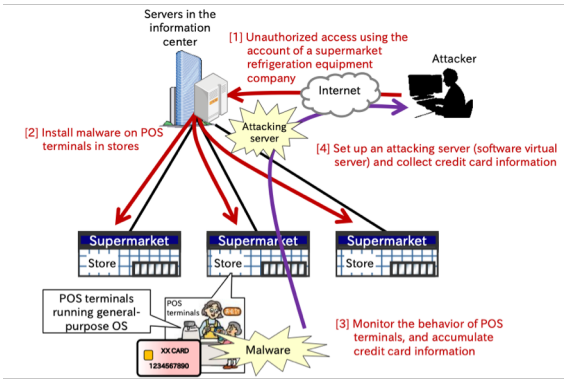
Problemas de *security*: Exemplos de incidentes

Period of media coverage	Device involved	Description
2013	Fetal monitor	At a medical center in the U.S., fetal monitoring devices were infected by malware and responses of these devices were delayed.
2014	ATM	An attack method was found that used smartphones to connect to the internal unit of an ATM via USB to cause virus infection, enabling cash withdraw from the ATM simply by cell-phone text-messaging.
2015	Infusion pump	A vulnerability was found in microcomputer controlled pumps that automatically infuse medicinal solutions into patients, which could allow changing the upper and lower limit of medicinal solutions through networks.

Outro exemplo de violação de *security*

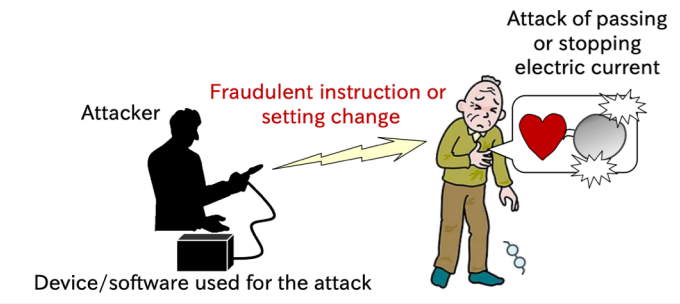
- Roubo de grandes quantidades de informação devido a infecção de terminais POS por malware

In 2013, it was found that POS terminals of a large retail chain in the U.S. were infected by malware (malicious software), and credit card information of 40 million customers and personal information of 70 million customers were leaked.



Exemplo onde *safety* e *security* são afectados

- Pacemakers cardíacos podem ser parados via wireless



In 2012, a U.S. researcher published an experiment, showing that transmission equipment can make cardiac pacemakers deliver a fatal electric current to hearts or falsify software in the pacemakers from a distance of less than 10m.

O que vamos ver a seguir

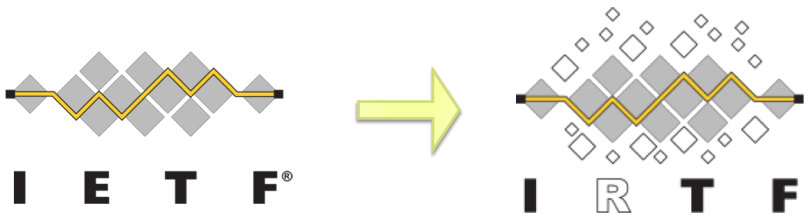
- Riscos e desafios de segurança em IoT
- Segurança na plataforma SmartThings

TÉCNICO LISBOA

Riscos e desafios de segurança em IoT

Estudo realizado pela IETF

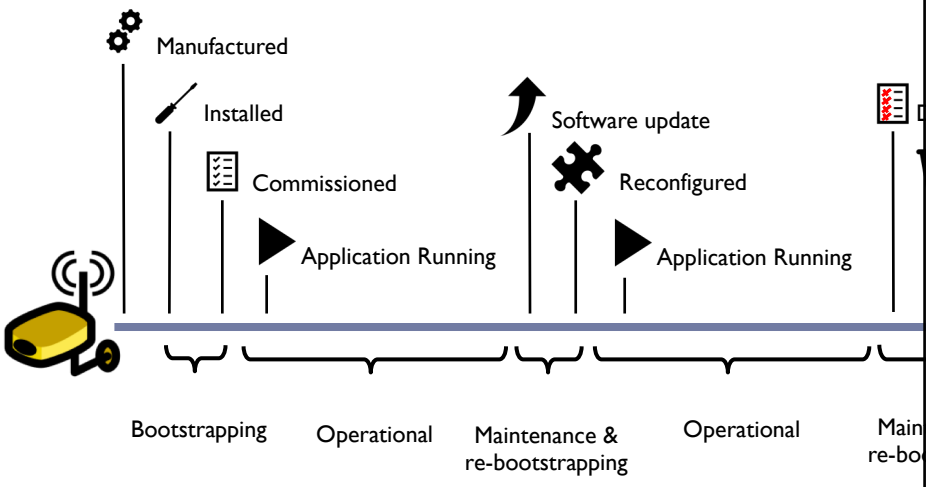
- Draft: Security Considerations in the IP-based Internet of Things
- Torna-se um IRTF Internet Draft em 2016
  - State-of-the-Art and Challenges for the Internet of Things Security
  - https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-16
- Também bom sumário das iniciativas de standardização



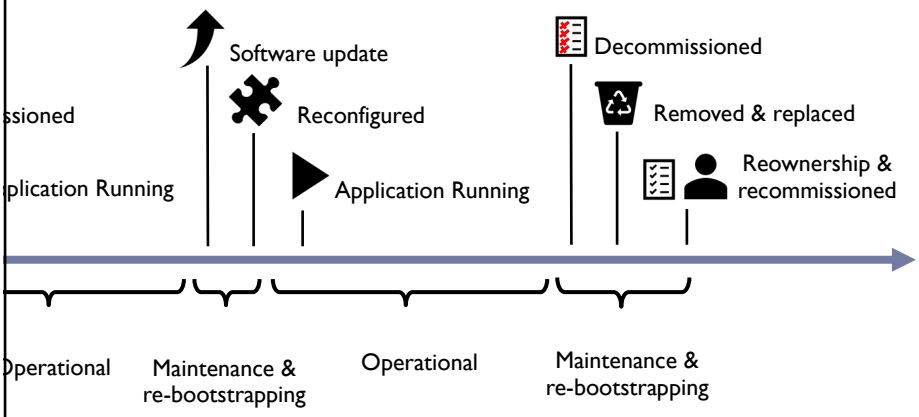
Dimensões da segurança em IoT

- Security
  - Confidentiality
  - Authentication
  - Integrity
  - Authorization
  - Availability

Vulnerabilidades no ciclo de vida das "coisas"

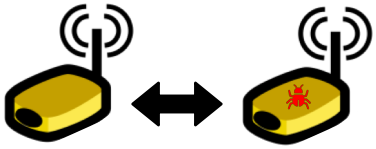


Vulnerabilidades no ciclo de vida das "coisas"



Ameaças de segurança para as "coisas"

- **Cloning of things**
  - Clone firmware, security configurations
  - Reverse engineer
  - Change functionality/add a backdoor

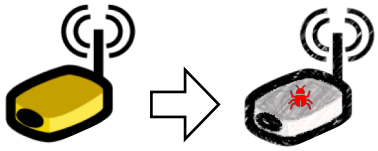


Manufacturing

Application Running

Ameaças de segurança para as “coisas”

- **Malicious substitution of things**
  - Different device is installed during Installation phase

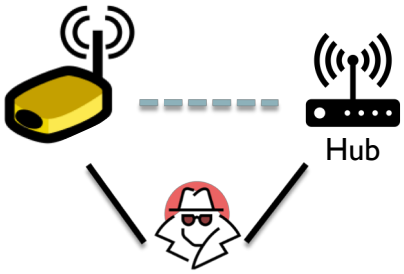


Ameaças de segurança para as “coisas”

- **Eavesdropping attack**
  - Security parameters exchanged in clear text
  - Device lifetime exceeds the cryptographic algorithms lifetime
  - Messages during T2T communication

Ameaças de segurança para as "coisas"

- **Man-in-the-middle attack**
  - Security parameters update exchanged in clear text
  - If device authentication is human-assisted, it may create a weak link



Commissioning

Application operational

Ameaças de segurança para as "coisas"

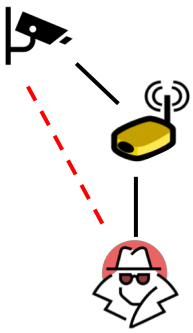
- **Firmware attacks**
  - During maintenance a new malicious firmware may be updated
  - Old firmware may contain security exploits

Software update

Application operational

Ameaças de segurança para as “coisas”

- **Privilege scalation**
  - Authentication system flaw
  - Low privileged user access higher priority resources

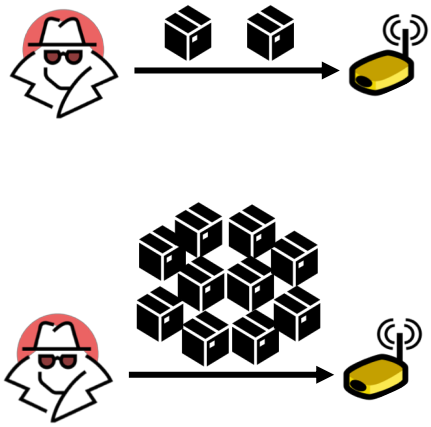


Ameaças de segurança para as “coisas”

- **Privacy threats**
  - Infer information based on device profile and messaging patterns
  - Also known as second channel attack

Ameaças de segurança para as "coisas"

- **Denial-of-Service attack**
  - Physically jamming the network medium
  - Constrained devices are more vulnerable
    - Resource exhaustion
  - Compromised devices used in a Distributed DoS

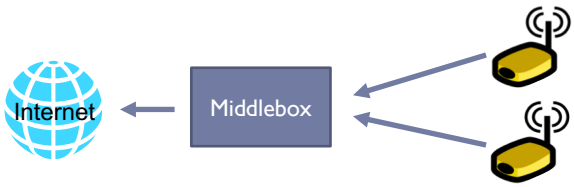


Desafios para IoT segura

- **Resource constraints**
  - Lossy and low-bandwidth communication channels
    - Possible DoS exploit, due to losses and retransmissions
  - Scarce processing and memory capacity limits the usage of resource expensive cryptographic primitives
    - Efforts in more efficient cryptography

Desafios para IoT segura

- **End-to-end security, protocol translation, and the role of middleboxes**
  - Sender to receiver confidentiality and integrity
    - Encryption commonly used
    - Gateways can't change or access the data
  - Constrained IoT networks uses different protocols that may needs translation at middleboxes
    - Middleboxes must access the message being sent (no end-to-end security)

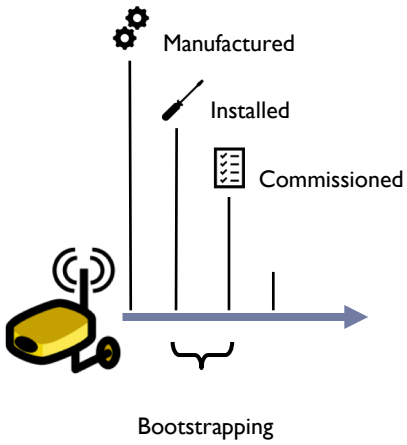


Desafios para IoT segura

- Solutions for end-to-end security challenge
  - Share credentials with middleboxes
  - Selectively protecting vital and immutable packet parts within a message, may result in poor performance or poor security
    - Encrypt and integrity protect most of the message fields except those parts that a middlebox needs to read or change
  - Homomorphic encryption techniques
    - Limited to arithmetic operations
    - Not many libraries with good support yet

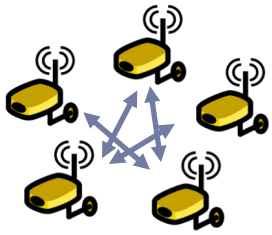
Desafios para IoT segura

- **Bootstrapping of a security domain**
  - Creating a security domain from unassociated IoT devices
  - Still an unresolved question



Desafios para IoT segura

- **Operational stage challenges**
  - Group Membership and Security
  - Group key solutions can be reused in IoT



Desafios para IoT segura

- **Mobility and IP network dynamics**
  - Expected that things will be attached to different networks during its lifetime (wearable sensors)

Desafios para IoT segura

- **Secure software update and cryptographic agility**
  - IoT devices are often expected to stay functional for several years and decades
  - Unattended operation
  - Software updates needed for new functionalities and security vulnerabilities
    - No incentive by manufactures
    - No source code available
    - Manual update
    - All the update threats
    - Source authentication

Desafios para IoT segura

- **Verifying device behavior**
  - How guarantee e that a device is doing what it claims
  - Devices may need to connect to the manufactures server, how can a user tell what data is being sent?
  - Challenging
    - Devices are not only constrained in resources but also in interface
    - Place of deployment will vary
    - It's a open question
- Some solutions
  - Manufacturer Usage Description (MUD) files [ID-MUD]
    - A first step in this direction
    - Describes what the device is supposed to the network
    - network monitoring service can then alert the user if the device does not behave as expected

Desafios para IoT segura

- **Testing and bug hunting and vulnerabilities**
  - It remains an open issue how classic quality assurance and bug testing will adapt to IoT devices
  - Also the combination of devices from different vendors may lead to dangerous network configurations

Desafios para IoT segura

- **Privacy protection**
  - Second channel attacks
- Defined as
  - awareness of privacy risks imposed by smart things
  - individual control over the collection and processing of personal information
  - awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere

Desafios para IoT segura

- Threats to user privacy
  - Identification - refers to the identification of the users and their objects
  - Localization - relates to the capability of locating a user and even tracking them
  - Profiling - is about creating a profile of the user and their preferences
  - Interaction - occurs when a user has been profiled and a given interaction is preferred (targeted marketing)
  - Lifecycle transitions - take place when devices are, for example, sold without properly removing private data
  - Inventory attacks - happen if specific information about (smart) objects in possession of a user is disclosed
  - Linkage - is about when information of two of more IoT systems is combined so that a broader view on the personal data is created
- Still an open issue

Desafios para IoT segura

- **Trustworthy IoT operation**
  - Flaws in the design and implementation of a secure IoT device
    - Same built in password for all devices (as Dr. Mosse mentioned about routers)
  - Tools to find IoT devices in the Internet
    - https://www.shodan.io/

OWASP IoT top 10 vulnerabilities 2018

https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

- 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

Três problemas sérios na plataforma SmartThings

- Como impedir que as aplicações tenham **acesso abusivo aos smartdevices** dos utilizadores?
- Como impedir que as aplicações efectuem **acções sem o conhecimento** dos utilizadores?
- Como impedir que diferentes aplicações **interfiram entre si causando resultados inesperados** pelos utilizadores?