

Desafios e perspectivas de Segurança Cibernética para Internet das Coisas

(Cyber Security Challenges and perspectives about IoT)

Robson de Oliveira Albuquerque
ENE/UnB

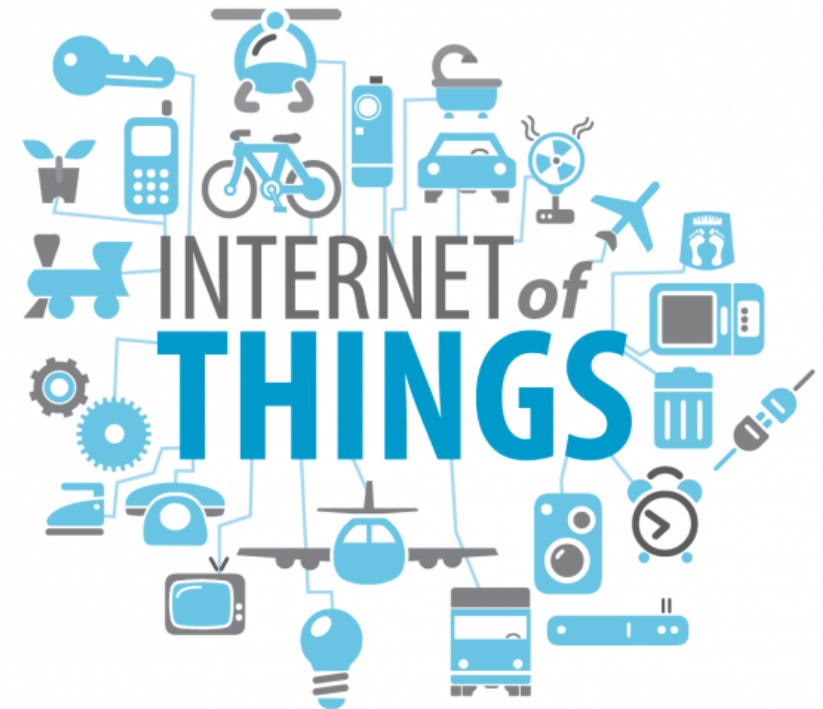
robson@redes.unb.br

Agenda

- **Internet of Things fundamentals;**
- **Security aspects regarding IoT;**
- **Some research results;**
- **Challenges and perspectives;**

IoT fundamentals

- What IoT is all about:
 - Things – devices, sensors, embedded systems, etc;
 - Communicate – networks, protocols and interactions;
 - Connections with external environment;
 - Contextual services provided by them;



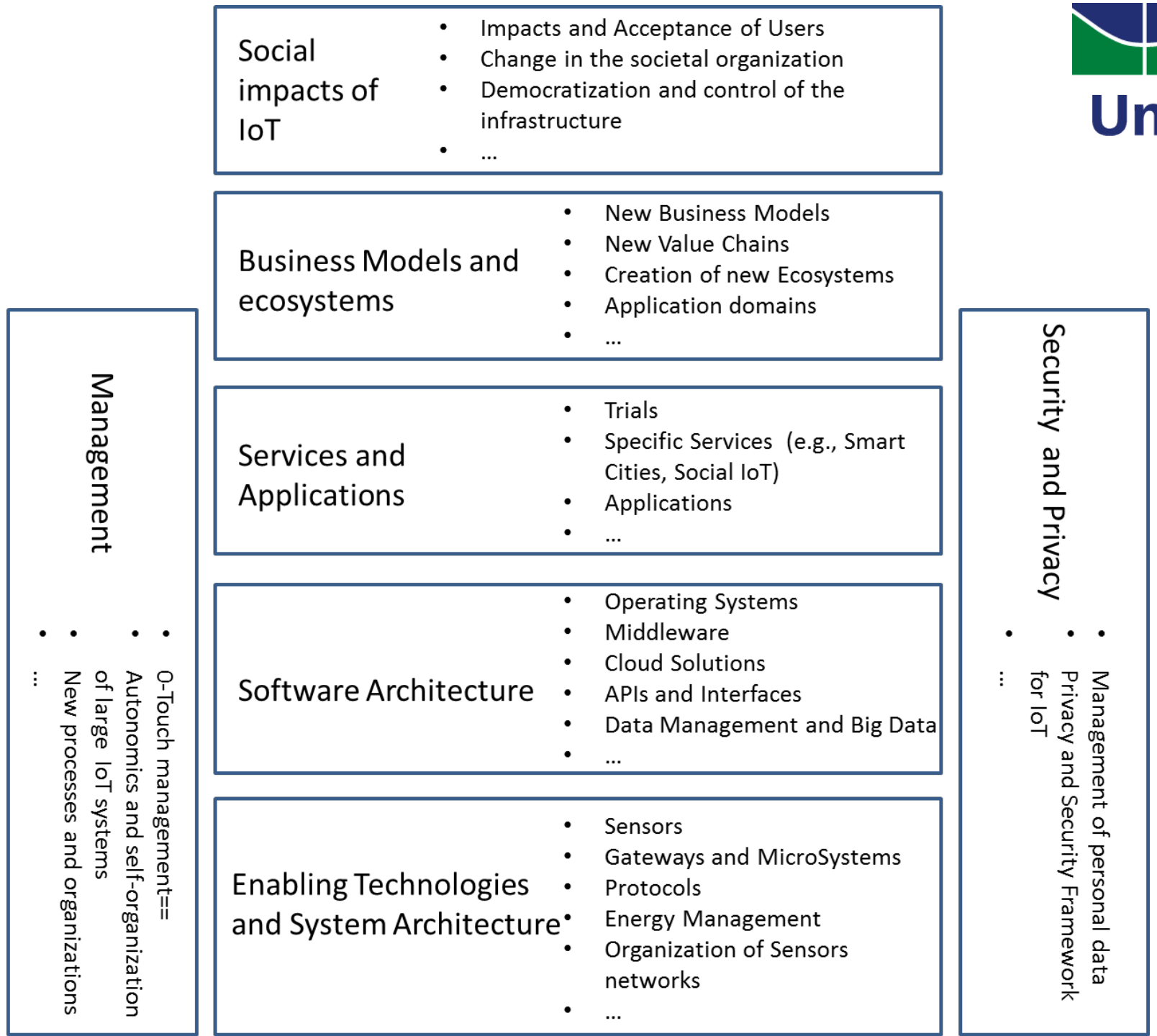
Source: <http://www.audiovisualstudio.es/el-internet-de-las-cosas-y-su-impacto-en-ferias-y-eventos/>

IoT fundamentals

- **There is not one unique definition of IoT;**
- **IEEE report:**
 - **Definition often depends on the particular vision of the proponent entity with respect to the assets of IoT that are considered more relevant**

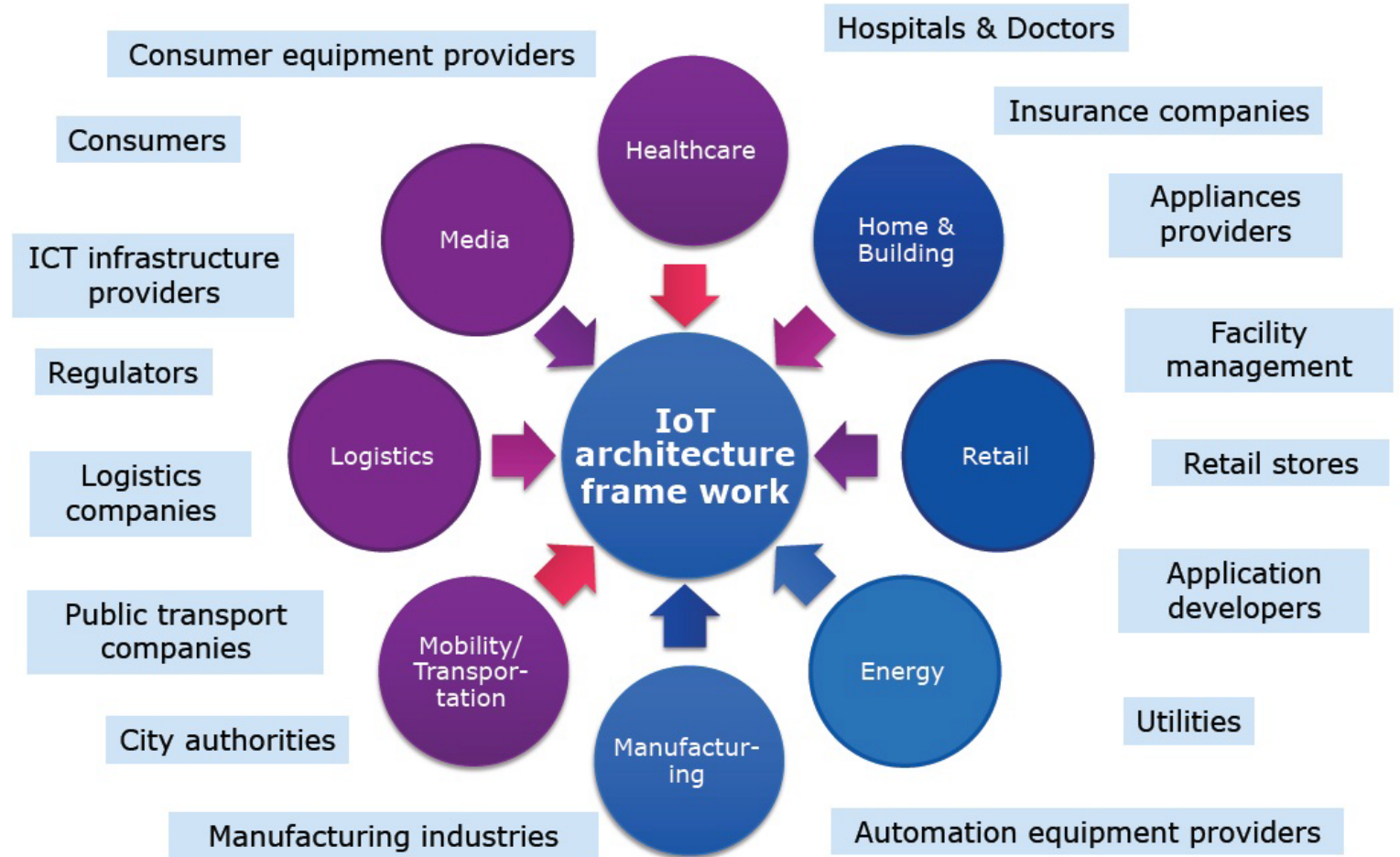
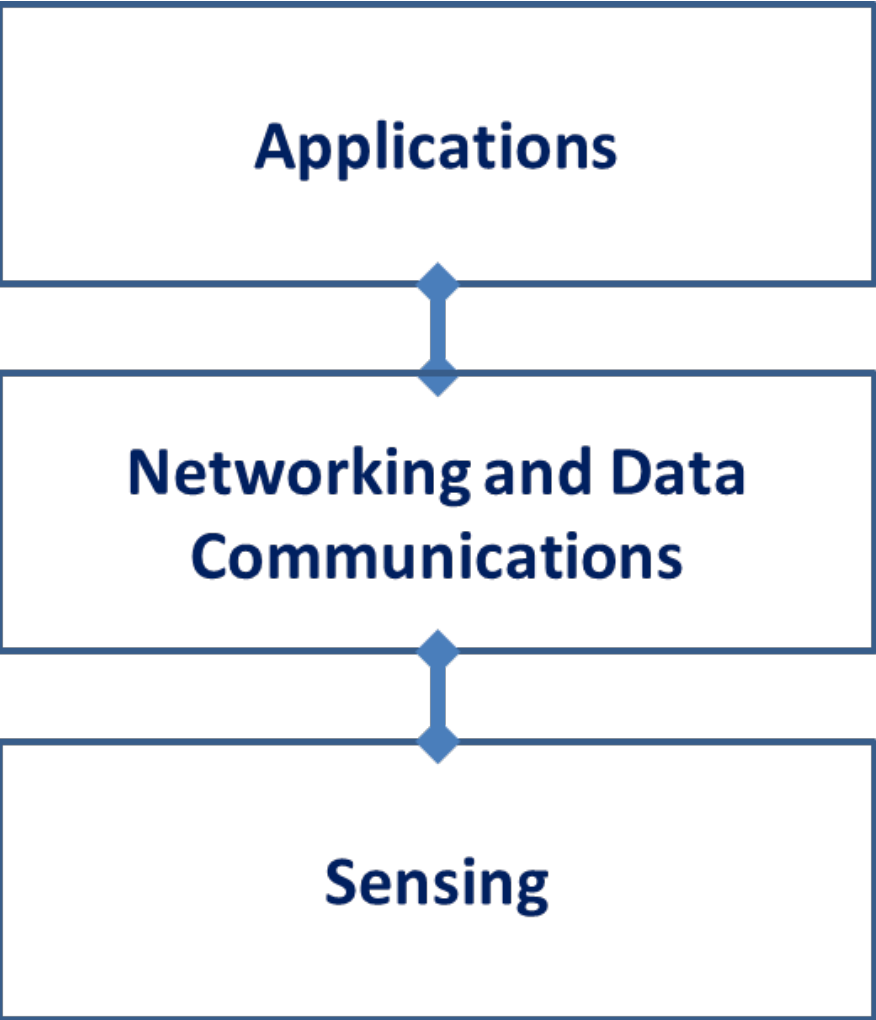
Source – IEEE Report – Towards a definition of the Internet of Things (IoT)
Revision 1 – Published 27 MAY 2015

• COMPLEX FRAMEWORK



Source – IEEE Report – Towards a definition of the Internet of Things (IoT) Revision 1 – Published 27 MAY 2015

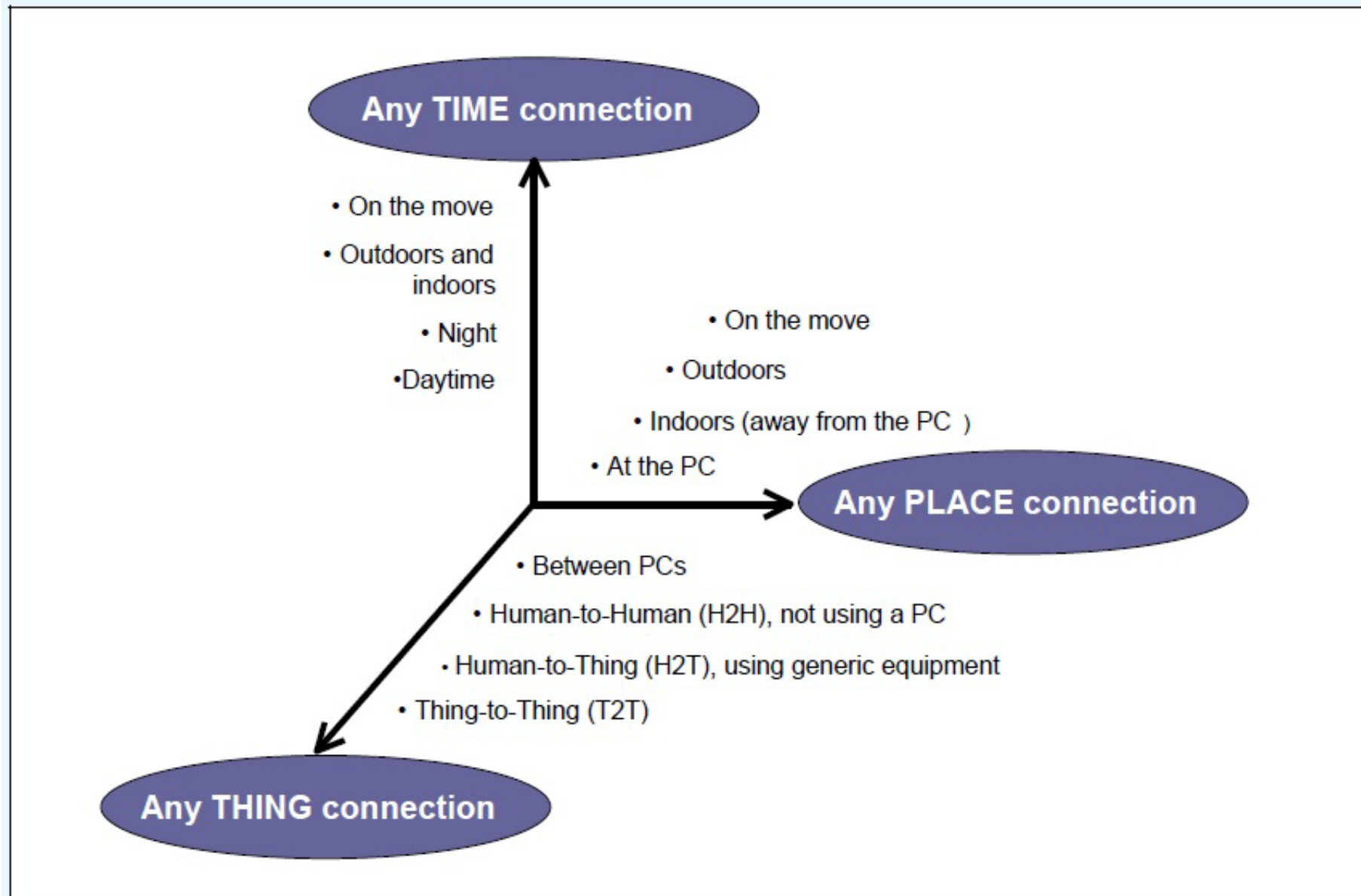
IoT fundamentals



Source – IEEE Report – Towards a definition of the Internet of Things (IoT)
 Revision 1 – Published 27 MAY 2015

IoT fundamentals

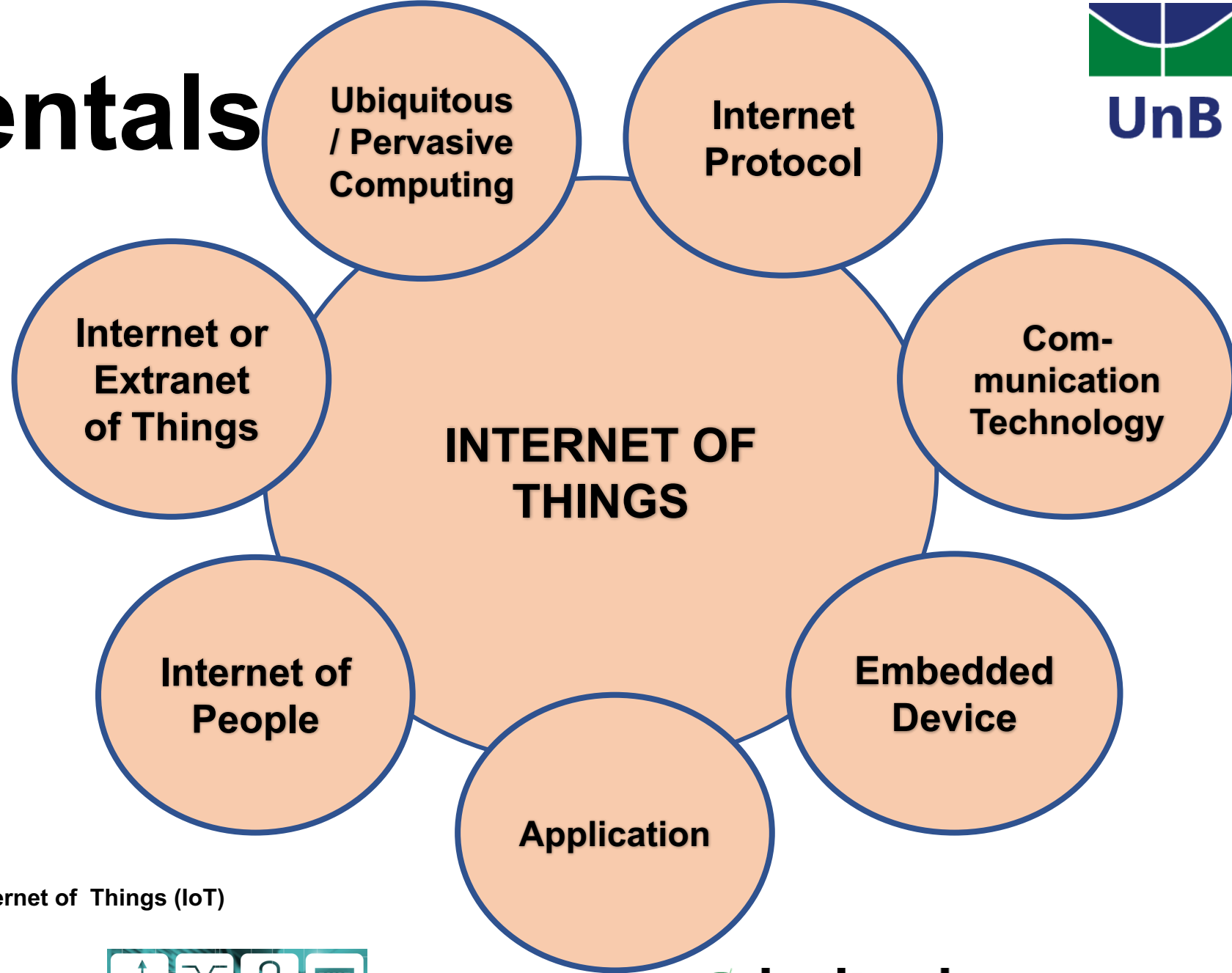
• ITU:



Source – ITU

IoT fundamentals

Internet of Things with other fields of research



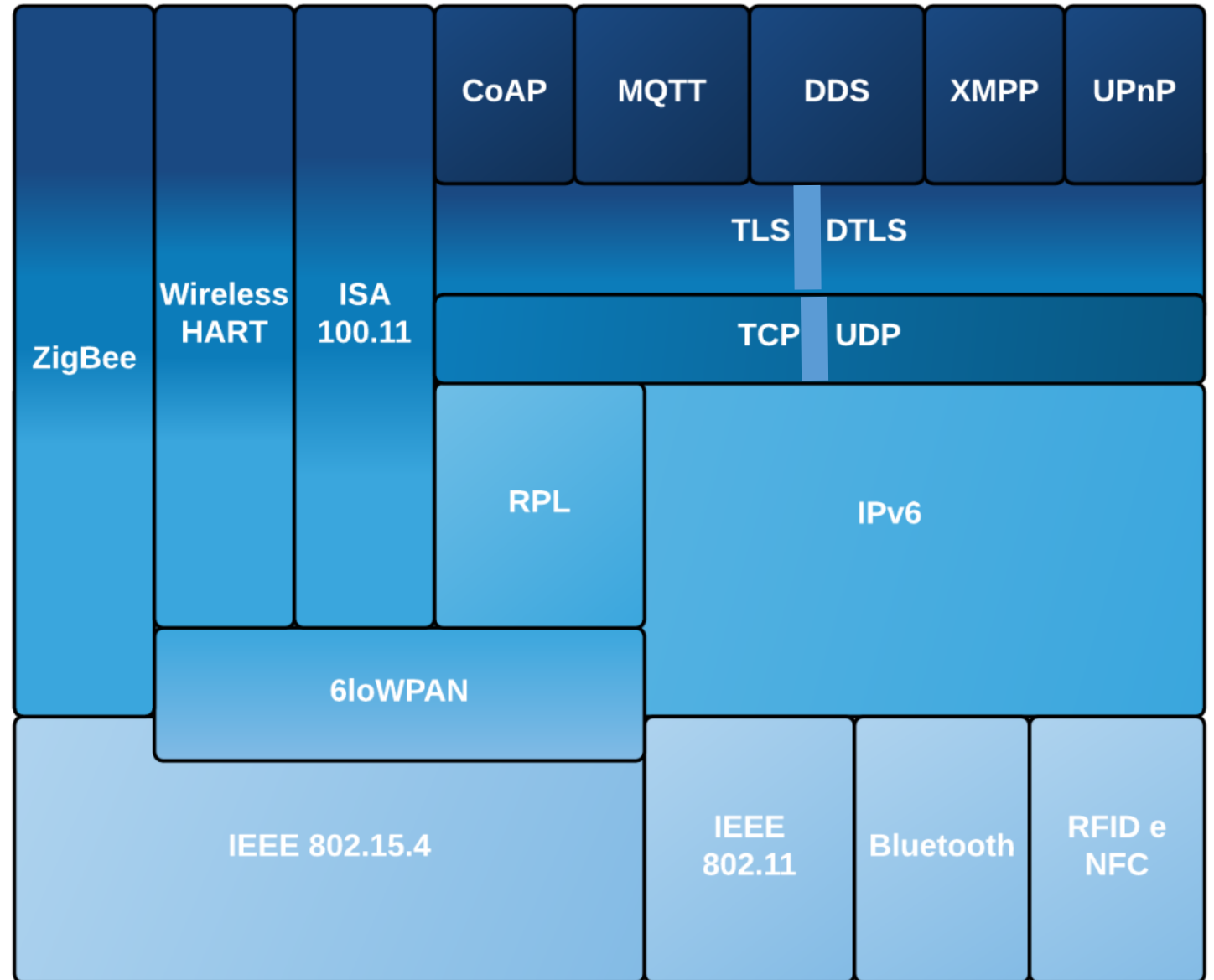
Source – IEEE Report – Towards a definition of the Internet of Things (IoT)
Revision 1 – Published 27 MAY 2015

Security aspects regarding IoT

- **IoT is not secure in many aspects:**
 - **Weak design of applications;**
 - **Weak protocols;**
 - **Weak firmware design;**
- **Of course there are limitations of the processing capabilities of IoT devices:**
 - **When the device is said to be "smart" there is a shift in the perspective;**

Security aspects regarding IoT

- Protocols used in IoT



Security aspects regarding IoT

- Some attacks on IoT protocols:

IEEE 802.11



Security aspects regarding IoT

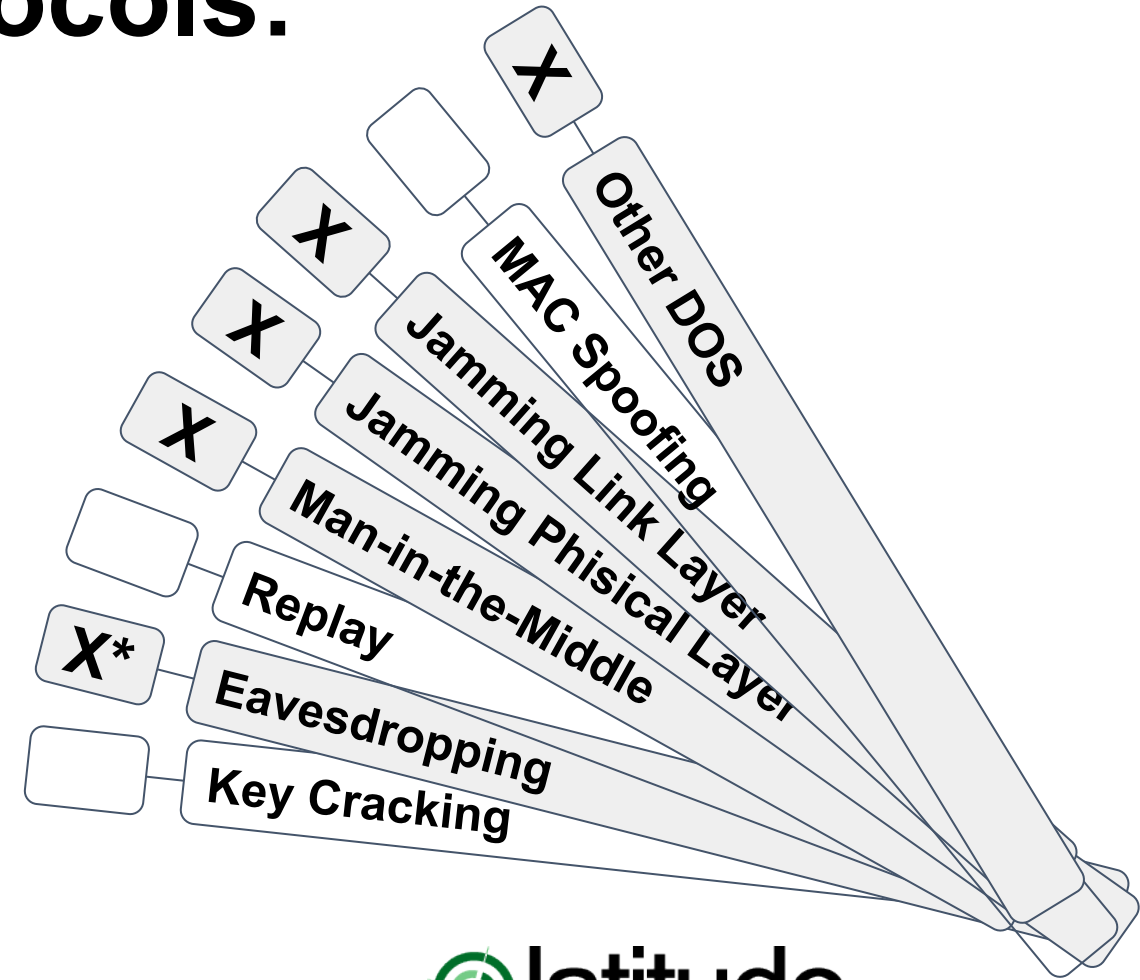
- Some attacks on IoT protocols:

Bluetooth



Security aspects regarding IoT

- Some attacks on IoT protocols:



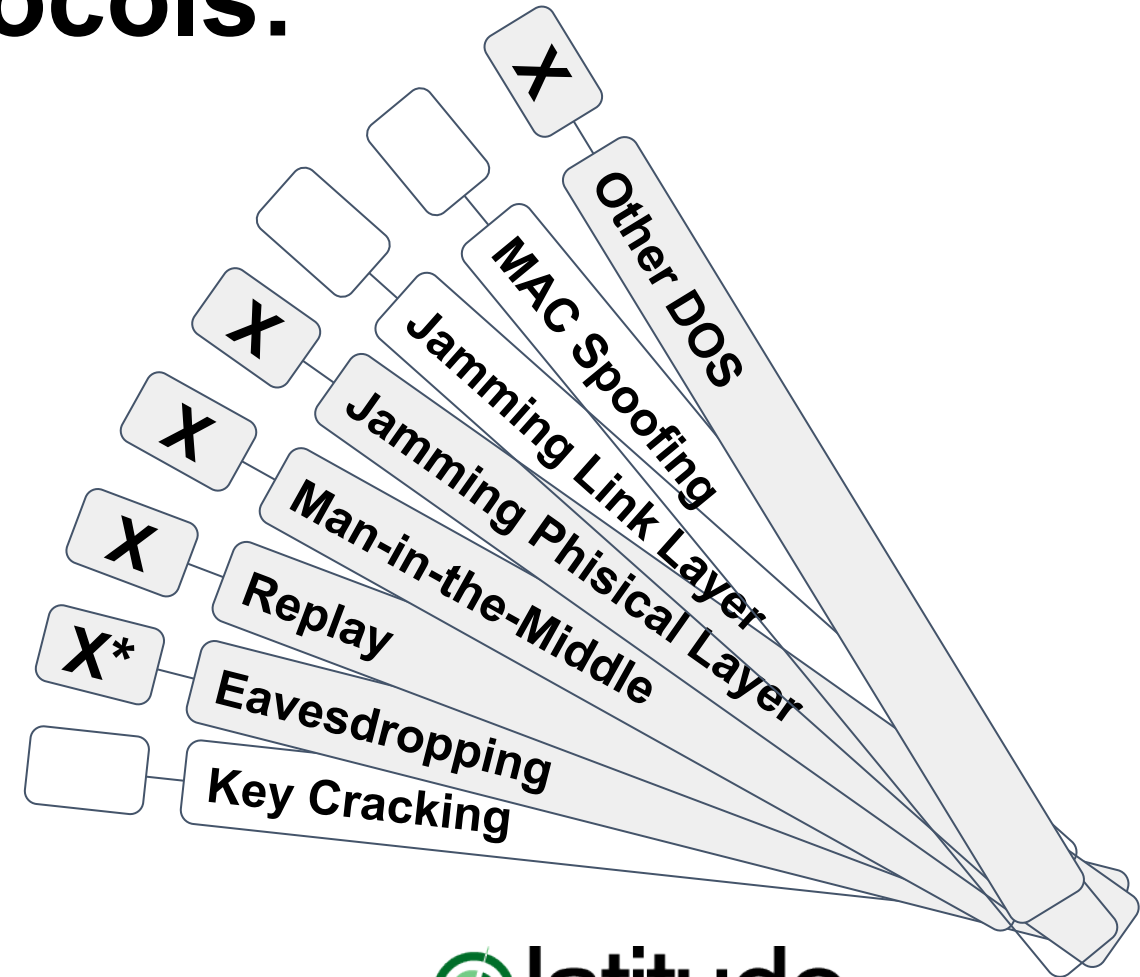
IEEE 802.15.4

Low-rate wireless personal area network, LR-WPAN

Security aspects regarding IoT

- Some attacks on IoT protocols:

RFID and NFC

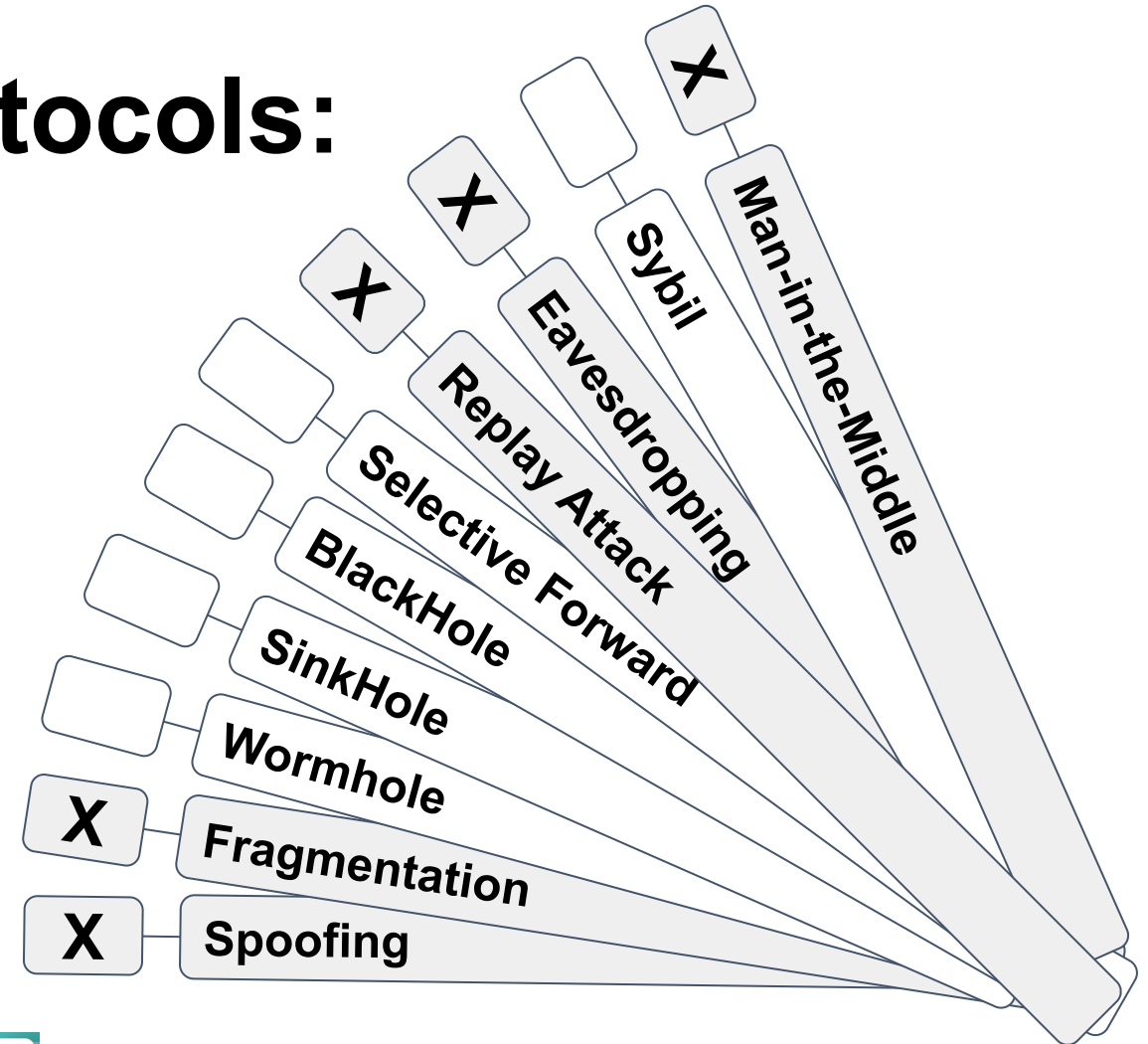


Security aspects regarding IoT

- Some attacks on IoT protocols:

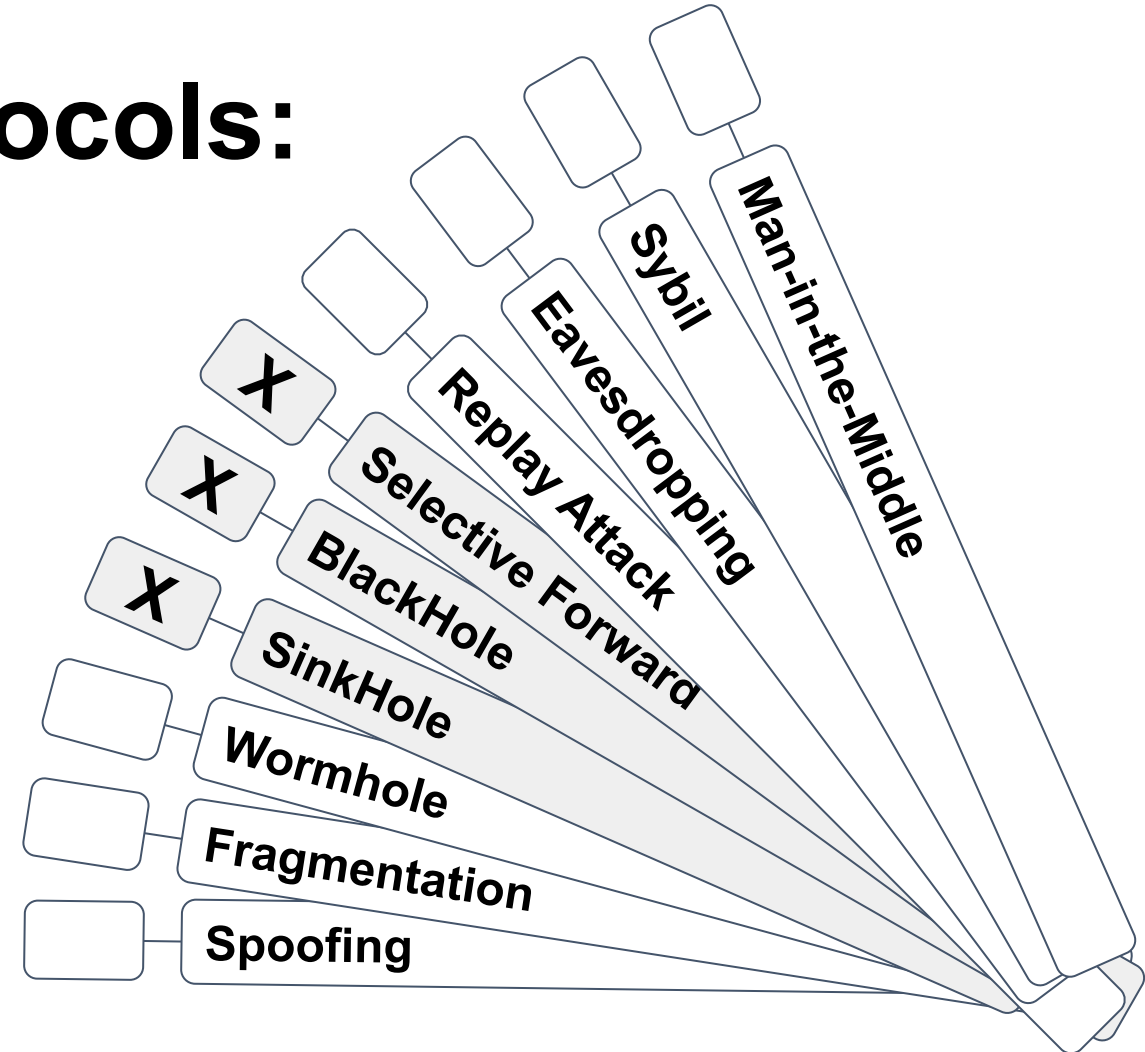
6LoWPAN

IPv6 over Low power Wireless
Personal Area Networks



Security aspects regarding IoT

- Some attacks on IoT protocols:



RPL

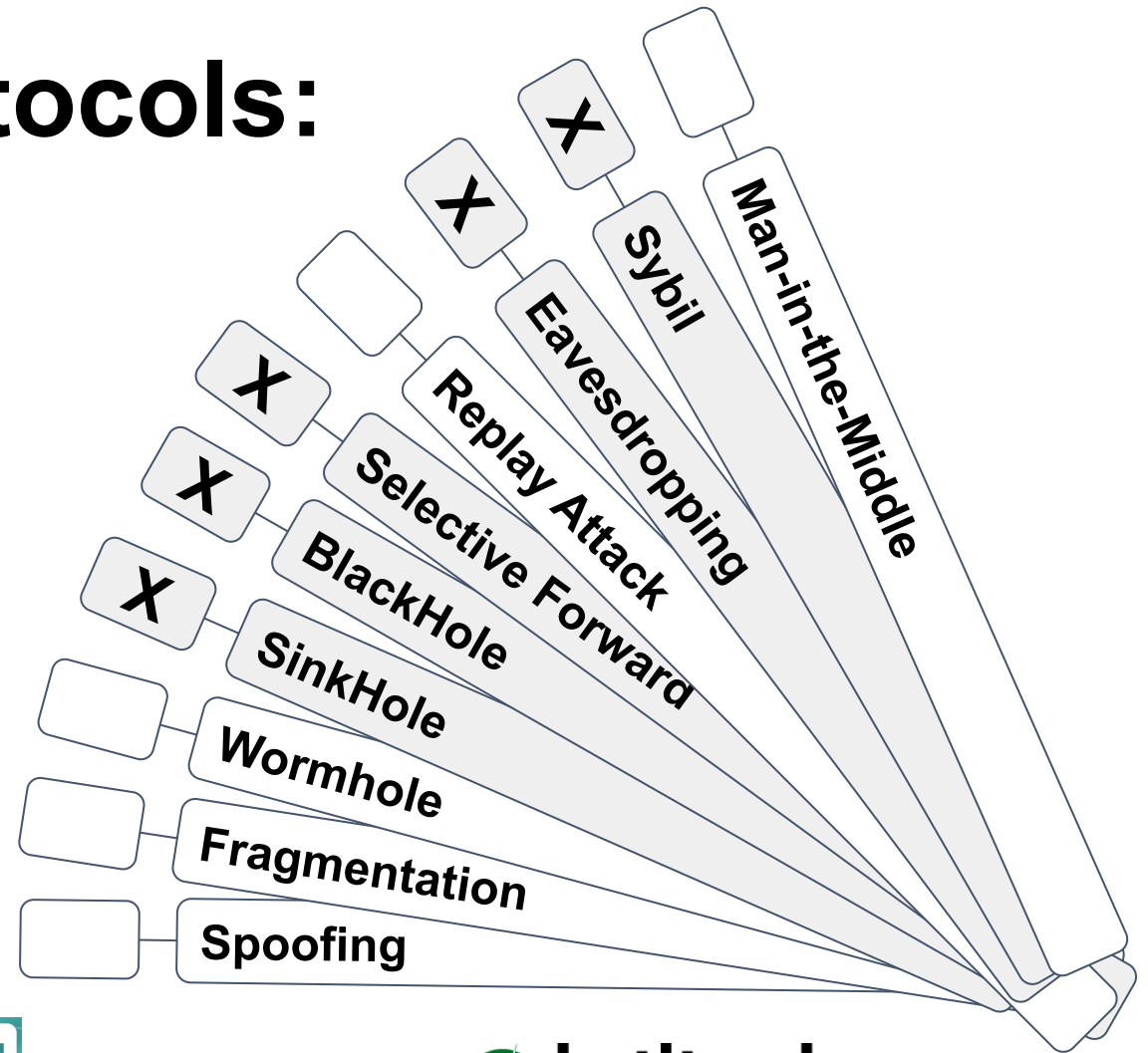
Routing over Low Power
and Lossy Networks

Security aspects regarding IoT

- Some attacks on IoT protocols:

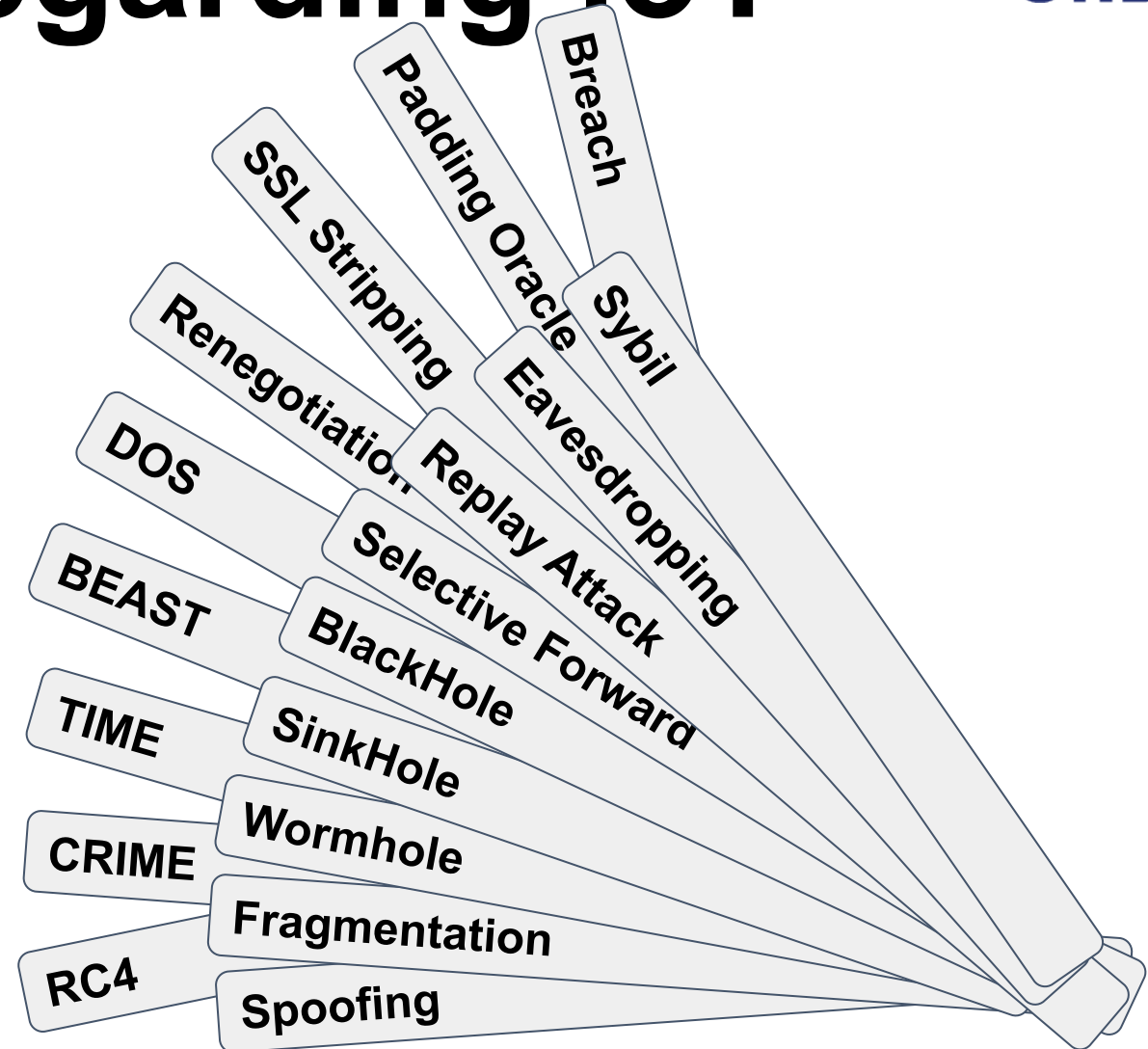
ZIGBEE

low-cost, low-power
wireless M2M networks



Security aspects regarding IoT

- Some attacks on IoT protocols:



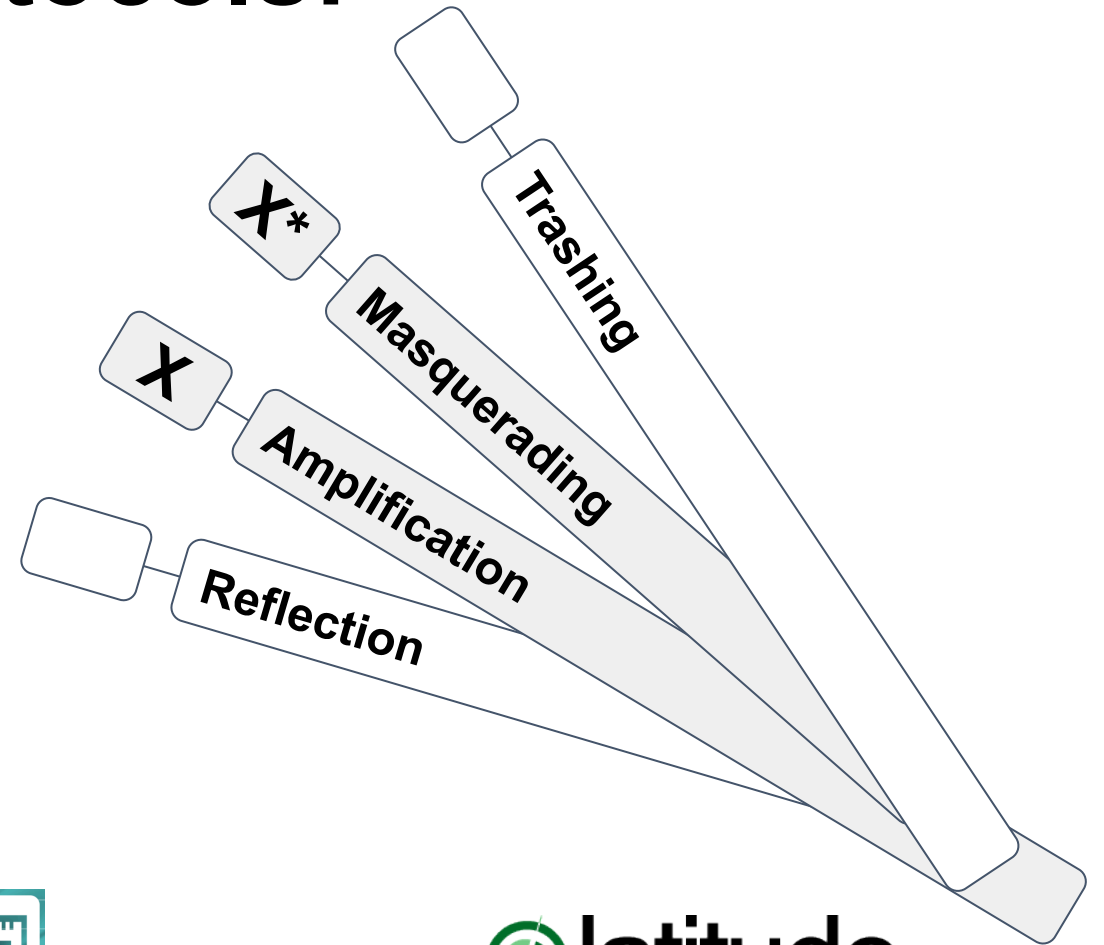
DTLS

datagram transport layer security

Security aspects regarding IoT

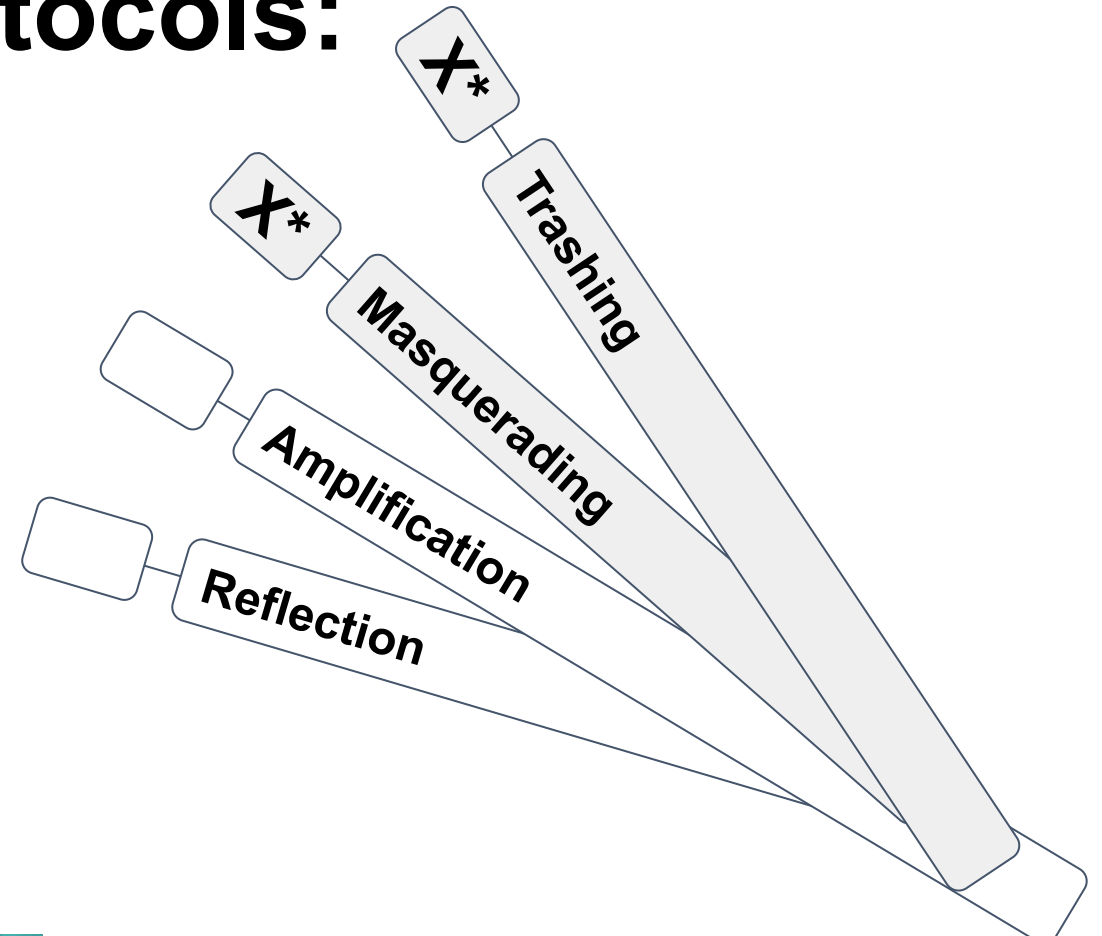
- Some attacks on IoT protocols:

CoAP
Constrained Application
Protocol



Security aspects regarding IoT

- Some attacks on IoT protocols:



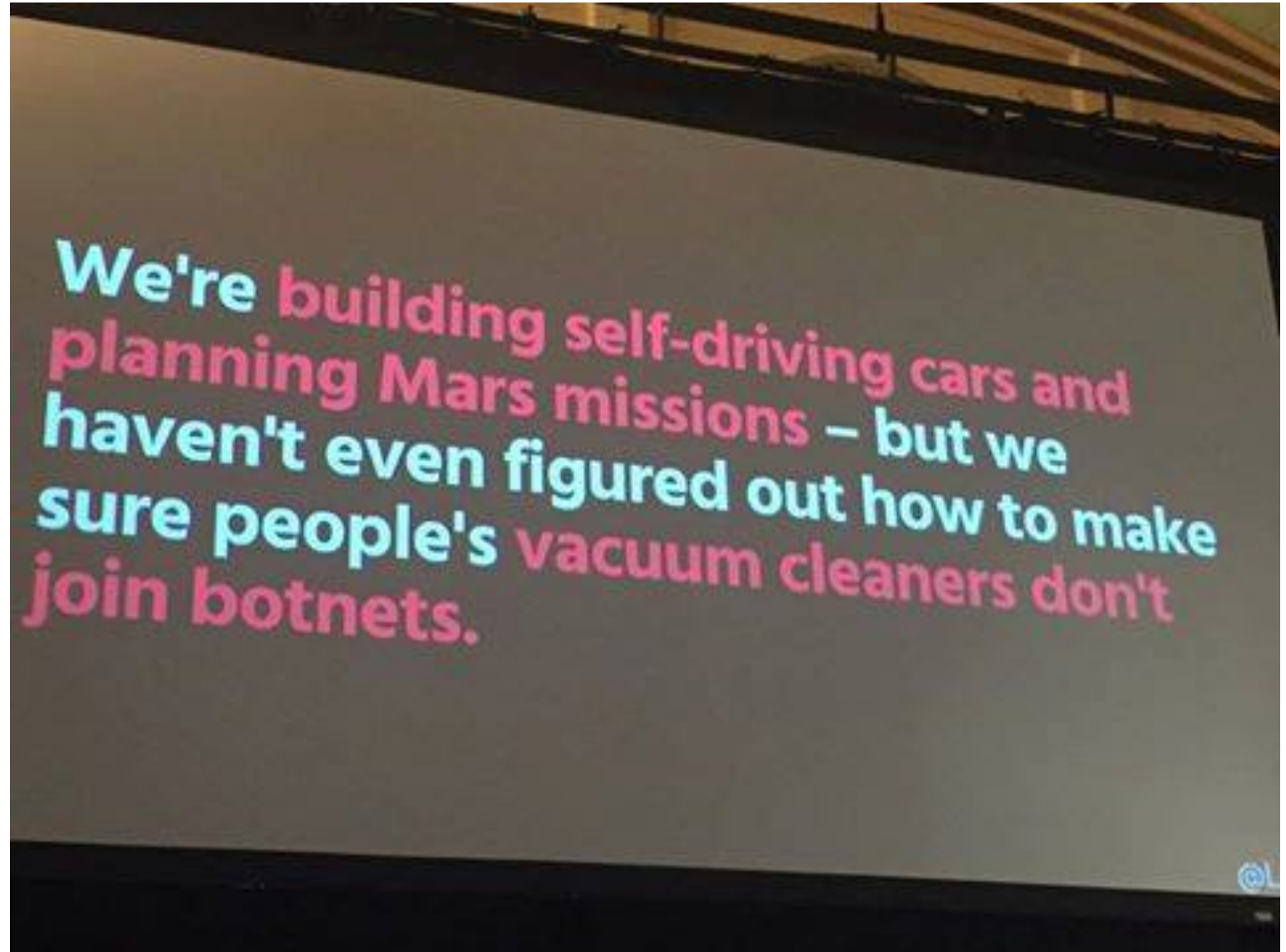
MQTT

Message Queue Telemetry
Transport (M2M)

Security aspects regarding IoT

- The use of **BOTNETS** in IoT:

Source:
<http://www.globalnerdy.com/2017/02/08/the-simplest-proof-that-information-security-isnt-a-priority/>



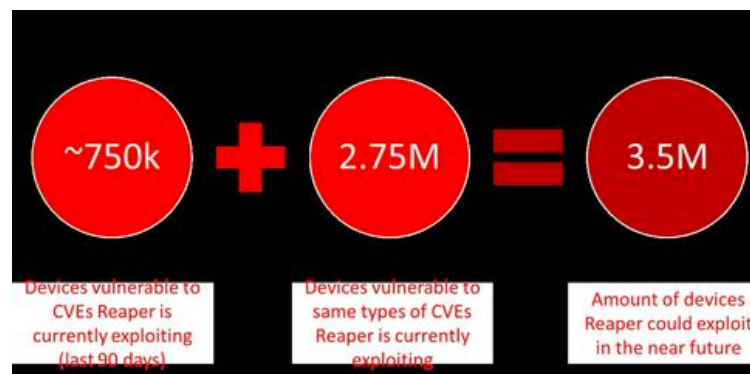
Security aspects regarding IoT

• IoT Botnets Know to be in activity:

BOTNET	POSSIBLE SIZE	ESTIMATES
MIRAI (ACTIVE)	145 K to 200 K	500 K
HAJIME (DORMANT)	300 K	Not known
REAPER (GROWING)	20 K to 40 K	Up to 3.5 M

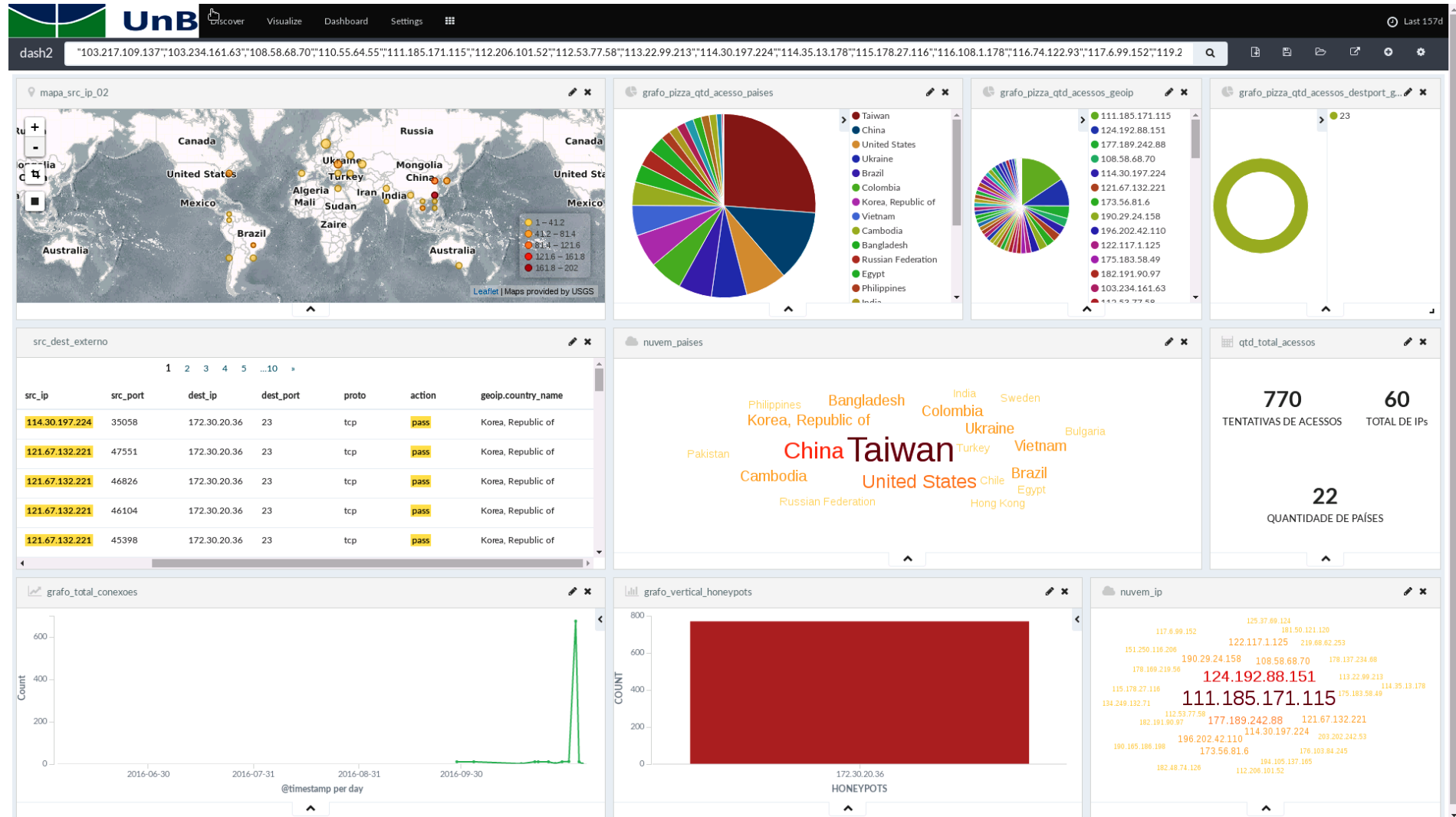
Source:

https://www.darkreading.com/partner-perspectives/f5/reaper-the-professional-bot-herders-thingbot/a/d-id/1330439?pidl_msgorder=asc/



Some research results

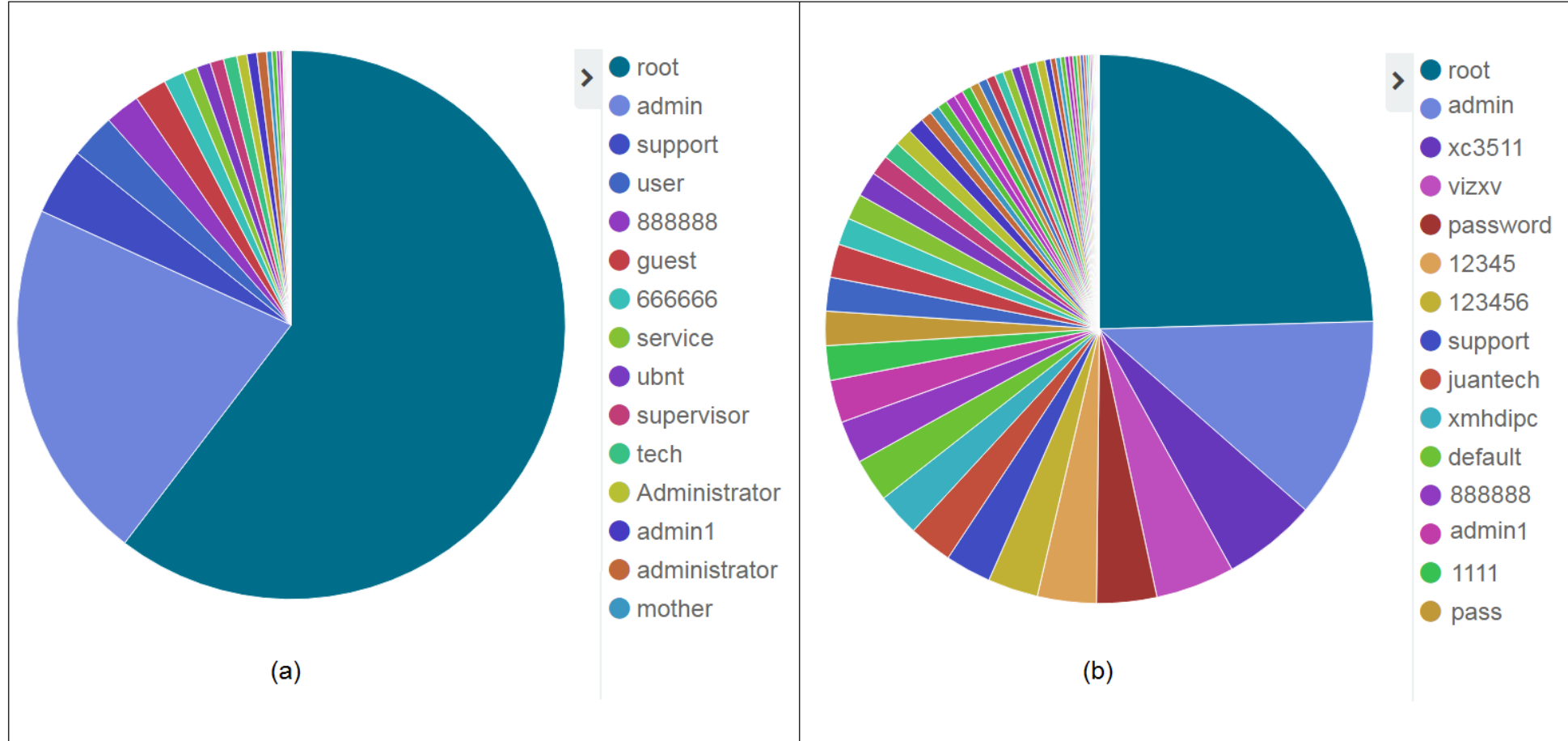
• In 2016 – Mirai Activity



Some research results

• In 2017 – Mirai Activity DPI analysis

Source:
<http://www.mdpi.com/2076-3417/7/10/1082>



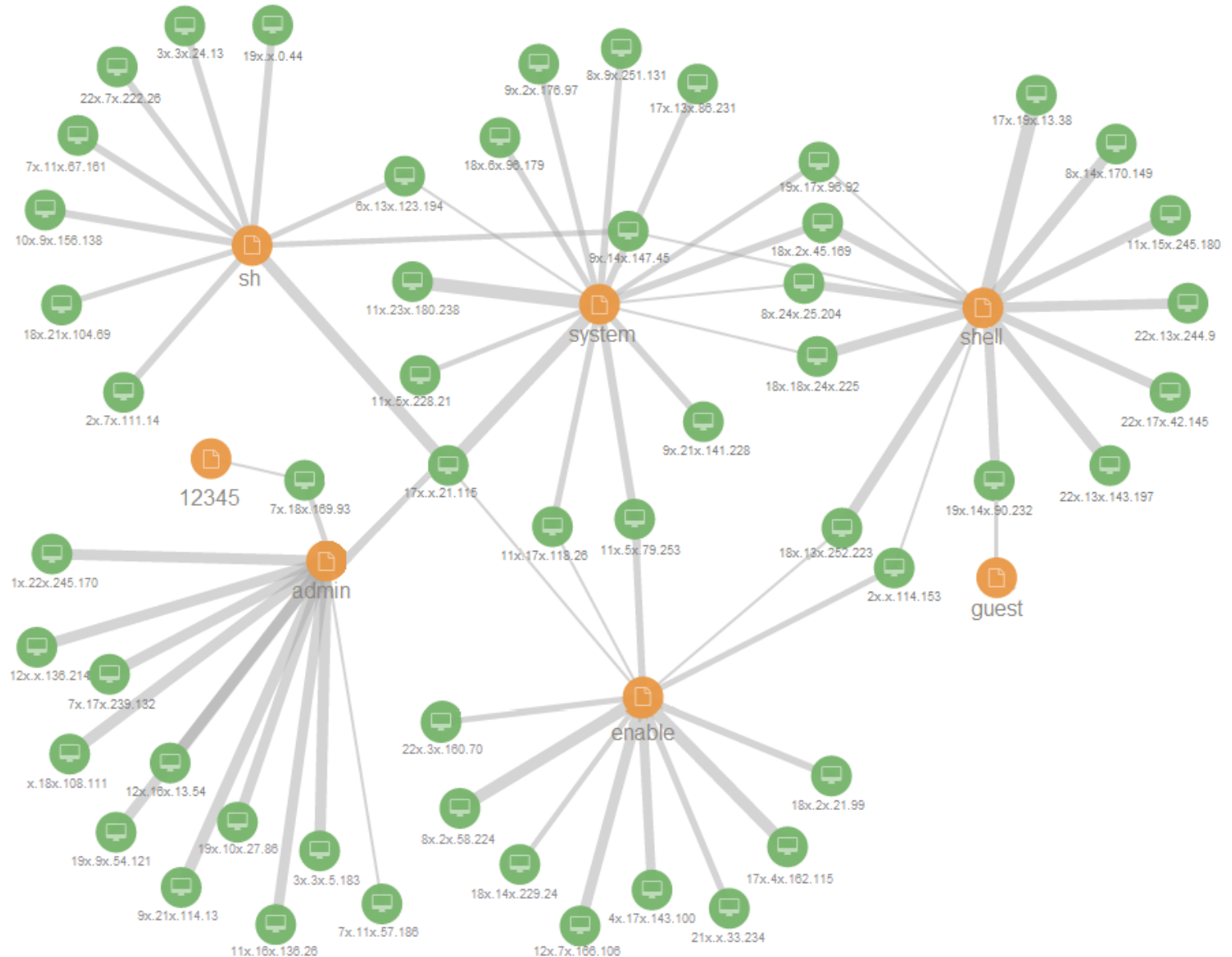
Users (a) and passwords (b) guessed by the Mirai botnet.

Some research results

• In 2017 –
Mirai
Activity

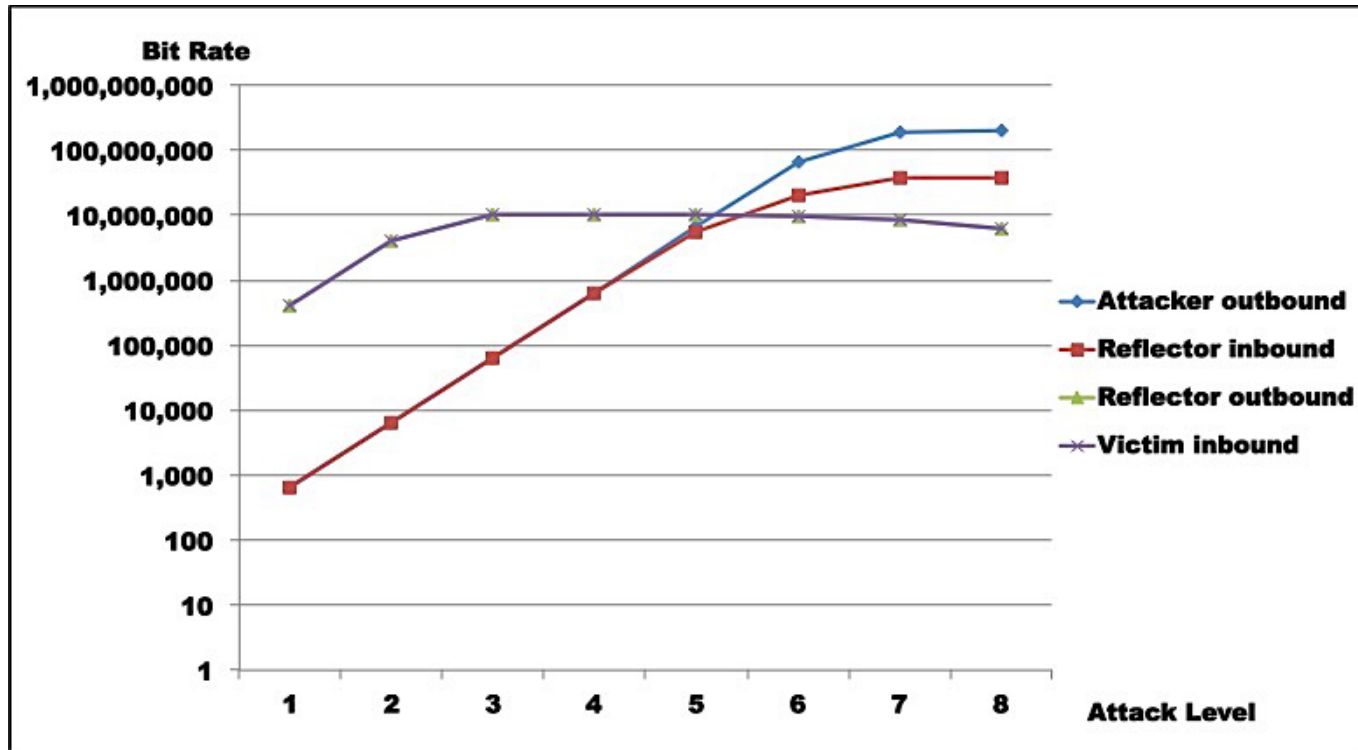
Modus Operandi

Source:
<http://www.mdpi.com/2076-3417/7/10/1082>



Some research results

• Amplification using SNMP



(b) Byte/s.

Level	Attacker		Reflector		Victim	
	Outbound	Inbound	Outbound	Inbound	Outbound	Inbound
1	82	82	50,013	50,013	50,013	50,013
2	816	819	502,124	502,124	502,124	502,124
3	8140	8140	1,307,921	1,307,921	1,307,921	1,307,921
4	80,659	80,548	1,282,255	1,282,255	1,282,255	1,282,255
5	815,064	697,994	1,279,351	1,284,195	1,279,351	1,284,195
6	8,163,136	2,554,131	1,187,994	1,187,994	1,187,994	1,187,994
7	23,215,614	4,829,191	1,058,325	1,057,670	1,058,325	1,057,670
8	24,815,635	4,808,938	805,020	804,460	805,020	804,460

Source: <http://www.mdpi.com:8080/1424-8220/16/11/1855>

Some research results

- IoT is also a Big Data Problem

Table 3. Number of devices for Kaa.

No. of Prod.	No. of Homes	Day	Month	Year
1	33,600	0.09 TB	2.86 TB	33.73 TB
2	63,492	0.17 TB	5.41 TB	63.74 TB
3	95,238	0.26 TB	8.12 TB	95.61 TB
4	142,857	0.39 TB	12.18 TB	143.41 TB

Source: <http://www.mdpi.com:8080/1424-8220/17/5/977>

Challenges and perspectives

- **Security:**
 - All levels in IoT design;
 - Tradeoff between usability versus security;
 - Sensors and applications used in Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) should be reviewed;
 - Security teams is not always true for IoT vendors;

Challenges and perspectives

- **Privacy:**
 - **Where is your data and who access it;**
 - **Eavesdropping;**
- **Big Data problem:**
 - **Small devices – huge amount of information generated;**
 - **To process and analyze it takes huge efforts;**
 - **Use of Cloud Solutions – problem is amplified;**

Challenges and perspectives

- **Regulation needs:**
 - **Governments should get involved when regulation is important;**
 - **Industry alone will not solve the IoT problem;**
 - **IoT policies and IoT markets;**
- **Research and Development:**
 - **Plenty of opportunities;**

Desafios e perspectivas de Segurança Cibernética para Internet das Coisas

(Cyber Security Challenges and perspectives about IoT)

Obrigado!

Robson de Oliveira Albuquerque
ENE/UnB

robson@redes.unb.br