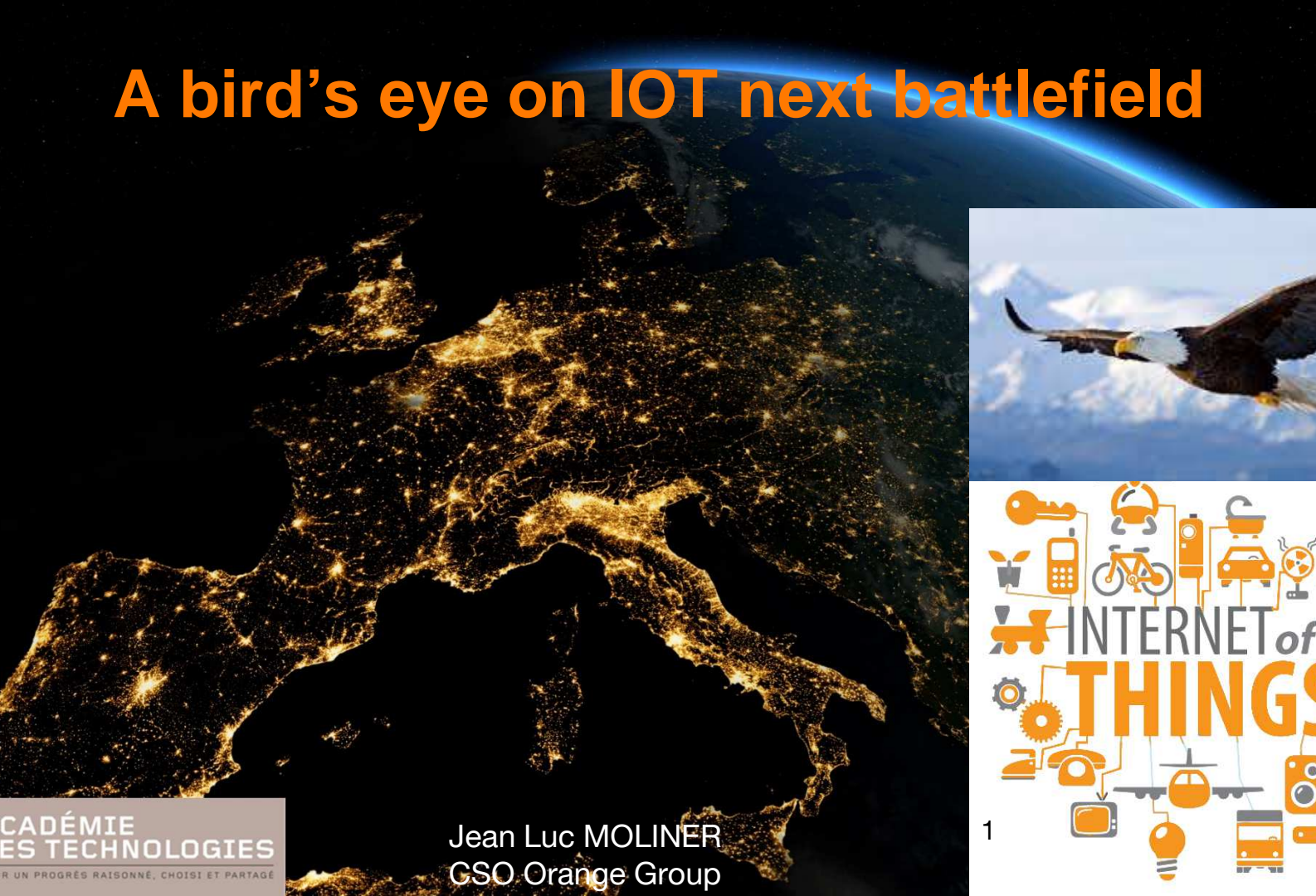


A bird's eye on IOT next battlefield



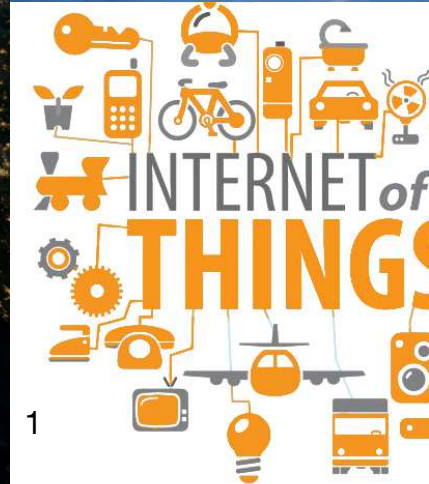
**ACADÉMIE
DES TECHNOLOGIES**
R UN PROGRÈS RAISONNÉ, CHOISI ET PARTAGÉ

Jean Luc MOLINER
CSO Orange Group

1

**ACADÉMIE
DES TECHNOLOGIES**
R UN PROGRÈS RAISONNÉ, CHOISI ET PARTAGÉ

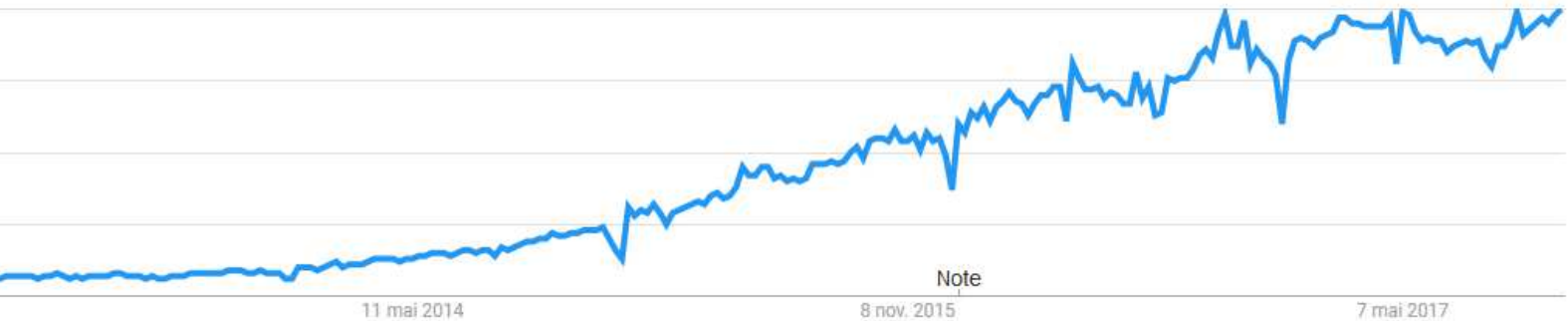
Jean Luc MOLINER
CSO Orange Group



Google Trends

« IoT » search theme from 2012 to 2017: x 15

l'intérêt pour cette recherche ?



Springer search on IoT : abundance of papers

Content Type	
Chapter	112,186
Conference Paper	36,986
Article	35,511
Reference Work Entry	2,027
Protocol	124
Book	78
Conference Proceedings	28
Book Series	1

agenda

1. What is IoT
2. Typical architecture
3. Markets
4. Some challenges
5. Security issues
6. Privacy challenges or nightmares ?

1- What is IoT

A Simple Explanation Of 'The Internet Of Things'



Jacob Morgan, CONTRIBUTOR

I write about and explore the future of work! [FULL BIO](#) ✓

Opinions expressed by Forbes Contributors are their own.

- Simply put, this is the **concept** of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes **everything** from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. As I mentioned, if it has an **on and off switch** then chances are **it can be a part of the IoT**.

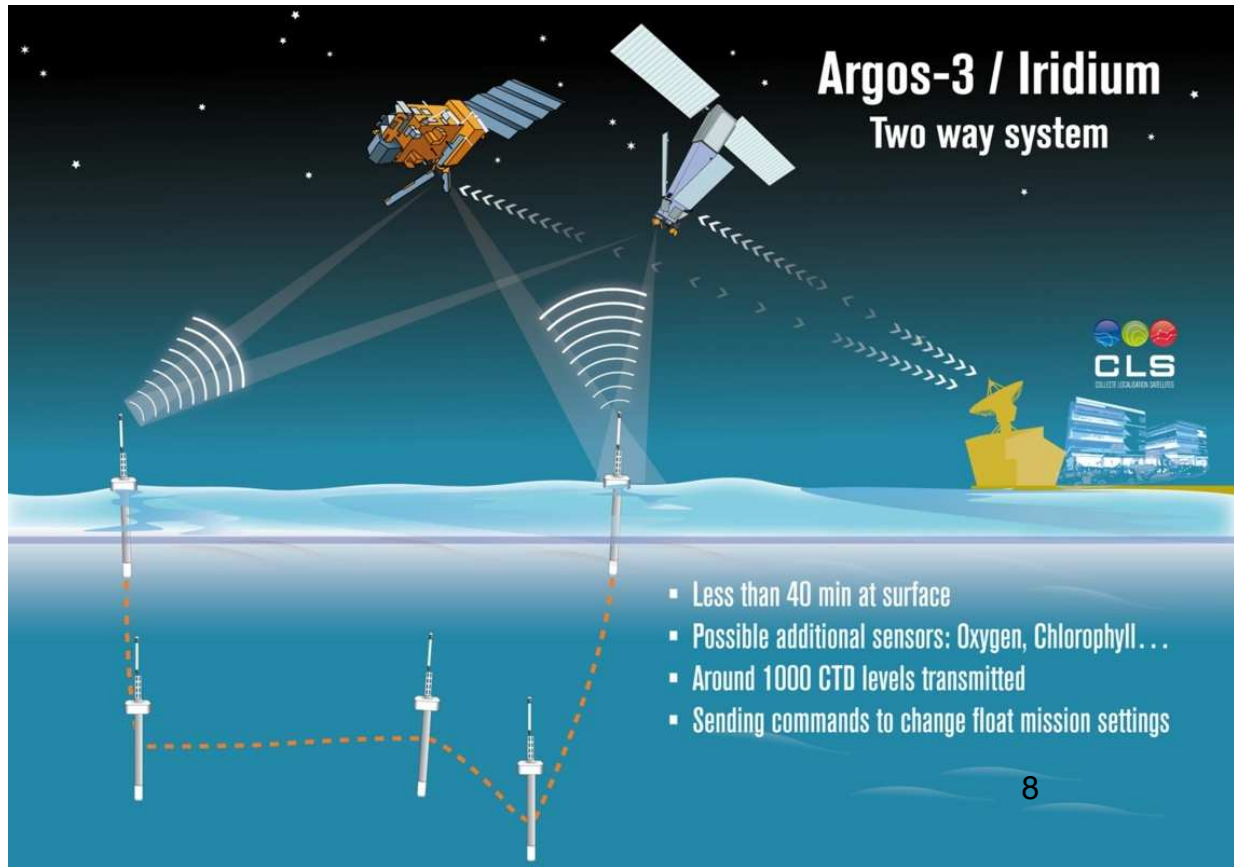
A connected object is:

“Sensor(s) and/or actuator(s) carrying out a specific function and that are able to communicate with other equipment. It is part of an infrastructure allowing the transport, storage, processing and access to the generated data by users or other systems.”

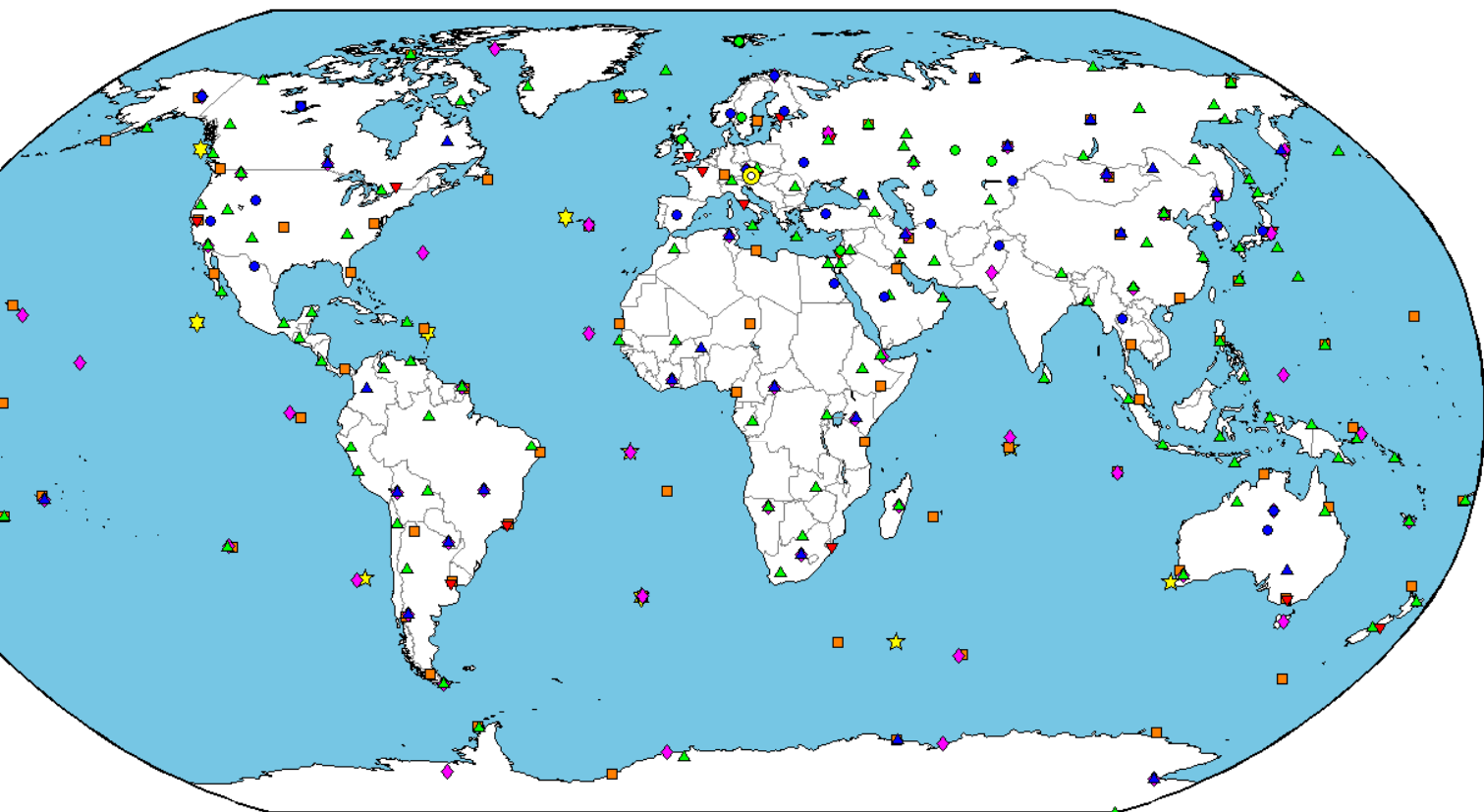
Then, a definition for the IoT would be:

“Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate.”

Good old time ...It was not IoT but network of interconnected sensors...ARGOS



INTERNATIONAL MONITORING SYSTEM



- Primary Seismic Array
 ● Auxiliary Seismic Array
 ◆ Infrasound Array
 ★ Hydroacoustic Station
 ■ Radionuclide Station
- ▲ Primary Seismic 3C Station
 ▲ Auxiliary Seismic 3C Station
 ★ T-Phase Station
 ▼ Radionuclide Laboratory
- International Data Centre
CTBTO Preparatory Commission

Taxonomy

1. Sensor communication: one way, two ways
2. Sensor energy: autonomous, battery powered, connected
3. Data Connectivity: wireless, physical connections to a LAN
4. Connectivity range: near field, short, medium, long
5. On board computing : yes/no
6. Consumables parts: yes/no
7. Asymmetric cryptography : yes/no
8. Software upgradeability: yes/no

2-Typical Architectures

T World Forum IoT Reference Model

Collaboration and Processes
(Involving People and Business Processes)



Application
(Reporting, Analytics, Control)



Data Abstraction
(Aggregation and Access)



Data Accumulation
(Storage)



Edge Computing
(Data Element Analysis and Transformation)



Connectivity
(Communication and Processing Units)



Physical Devices and Controllers
(The "Things" in IoT)

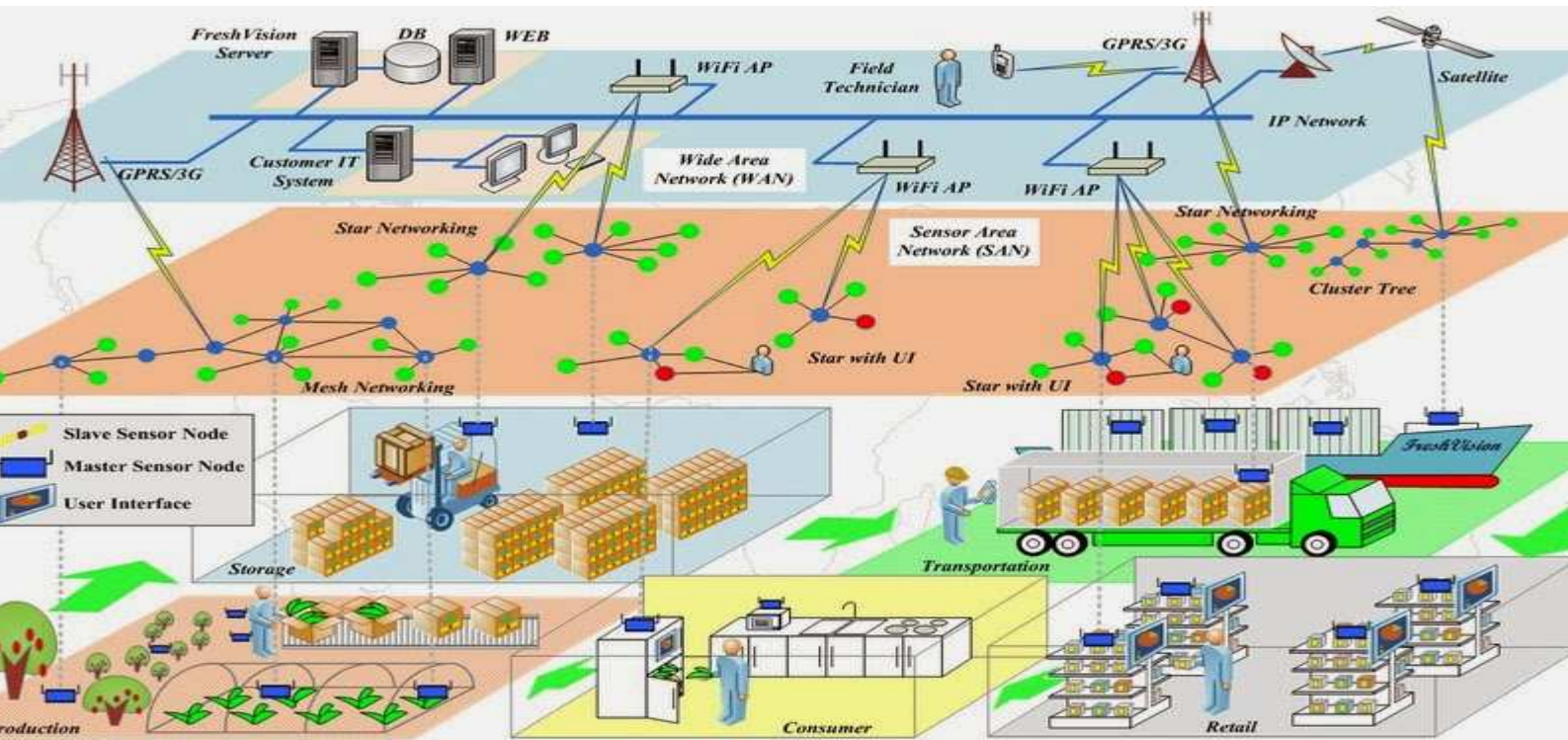


EDGE: Sensors, Devices, Machines,
Intelligent Edge Nodes of all types



Key Points

- IT-OT
- Decoupling Scalability Agility
- Interoperability
- Legacy Compatibility
- Analytics
- Integrated with the Enterprise



T End-to-End Architecture

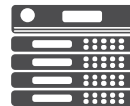
IOT APPLICATIONS
(ANY VERTICAL ENABLED BY SP)

SP SERVICES
(IDENTITY AND ACCESS, L7 FIREWALL,
INTEGRATED SERVICE POLICY, DNS, ANALYTICS)

SP NETWORKS
(CONNECTIVITY, LOAD BALANCING, NETWORK FIREWALL,
NETWORK POLICY, DNS, SUBSCRIBER DATA)

THINGS
(SENSORS, WEARABLES, IOT GATEWAY)

APP



3-Markets



Revenue Category Forecast

How do IoT revenues break down?

Services & Software will dominate

64% of IoT revenues in 2025

Security, analytics tools, business apps and software, consulting and integration

Connectivity revenues to stabilise

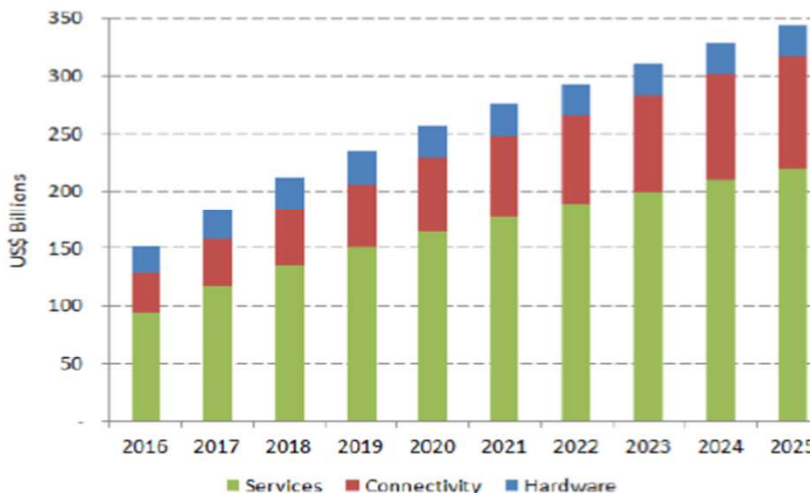
28% of IoT revenues in 2025

Includes network traffic, connectivity and service enablement

Hardware costs larger upfront, as economies of scale kick in, hardware % decreases

8% of IoT revenues in 2025

Includes modules, gateways, storage, servers, etc.



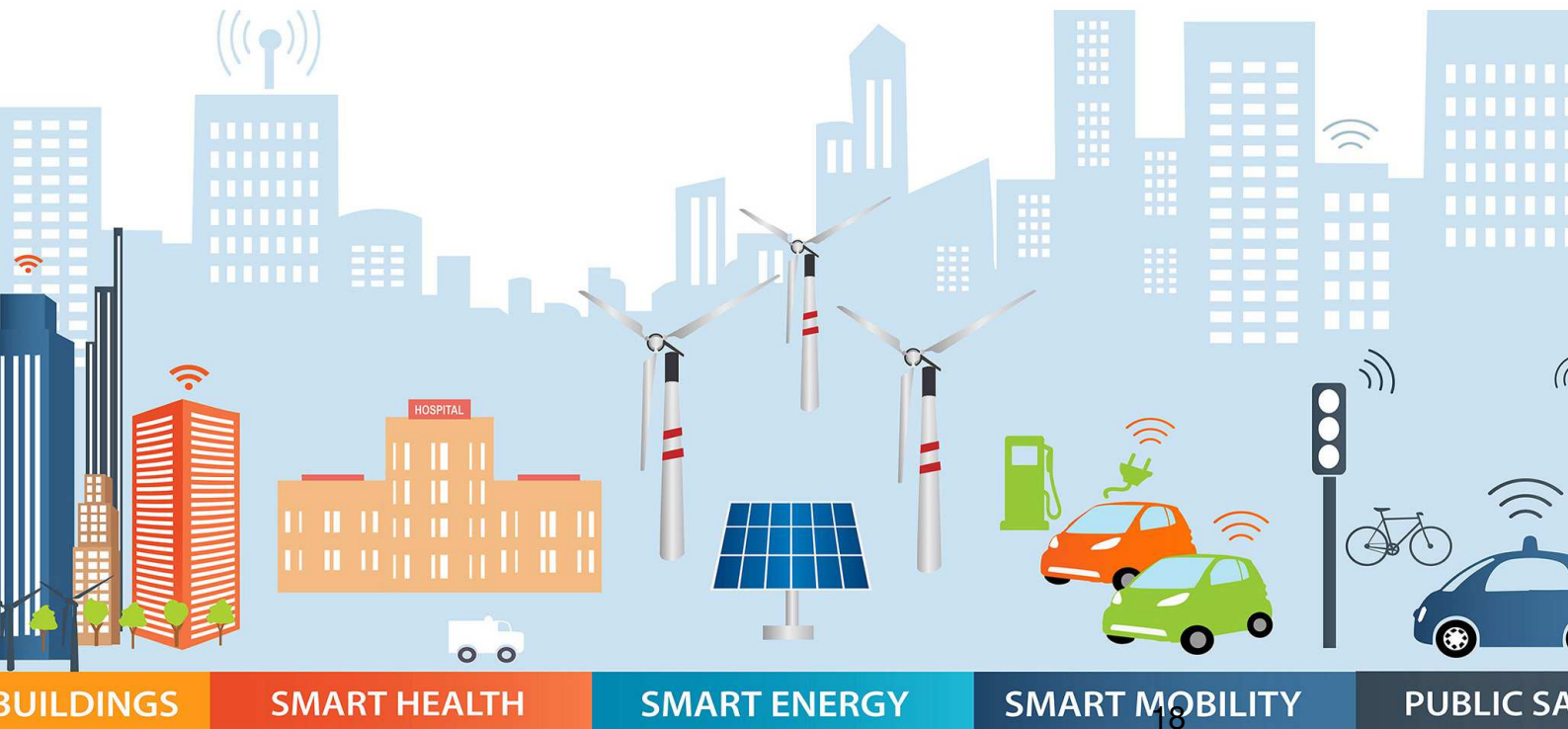
Source: IoT Strategies, April 2017

Markets segmentation

3-1 Industry at large



2 Smart city



3 Smart Grid (water, energy)

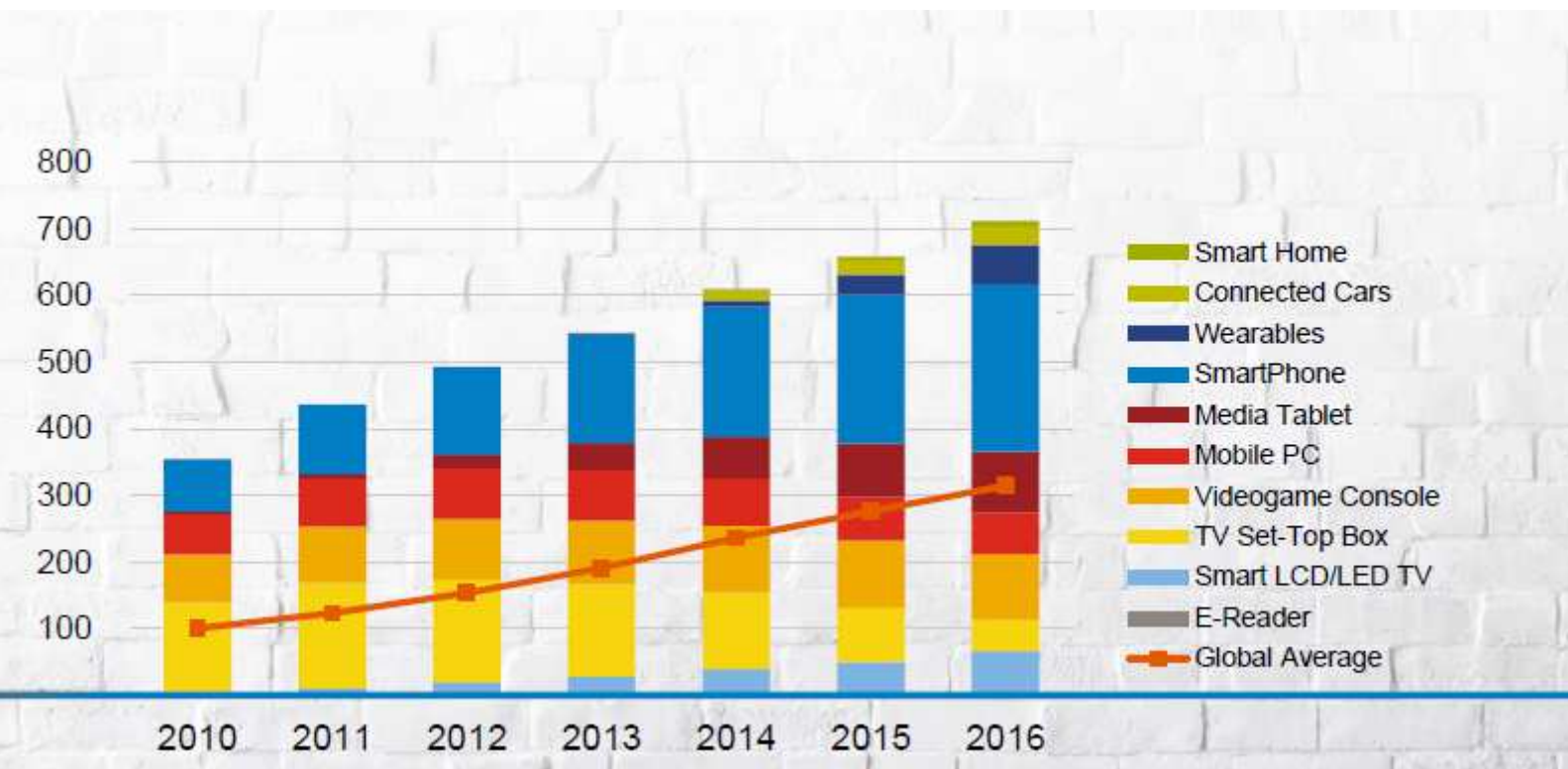


3 Home



3-4 Wearables





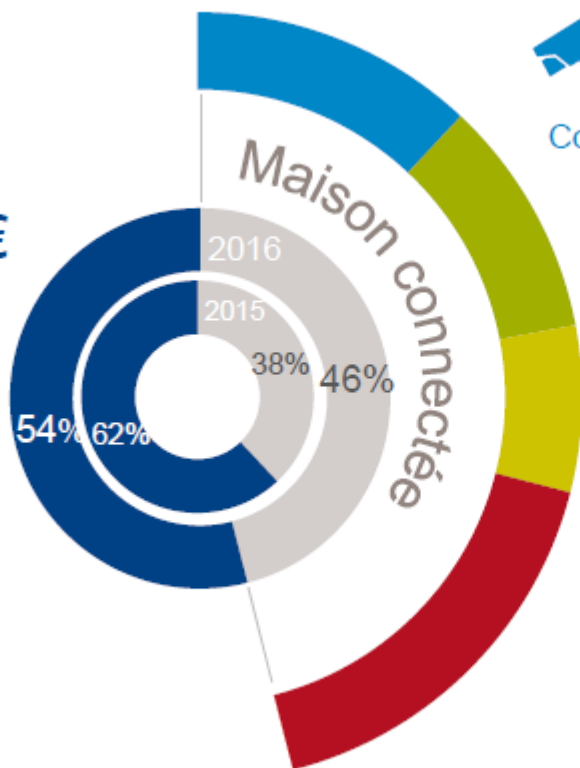
French market for Wearable & Market

251M.€

+20%



Wearable



Confort & sécurité

56M.€

+49%



Petit électro & santé

44M.€

x2,2



Réseau domestique

31M.€

+4%



Drones & divers

79M.€

+50%



Vertical Market Forecast

5 verticals **dominate**

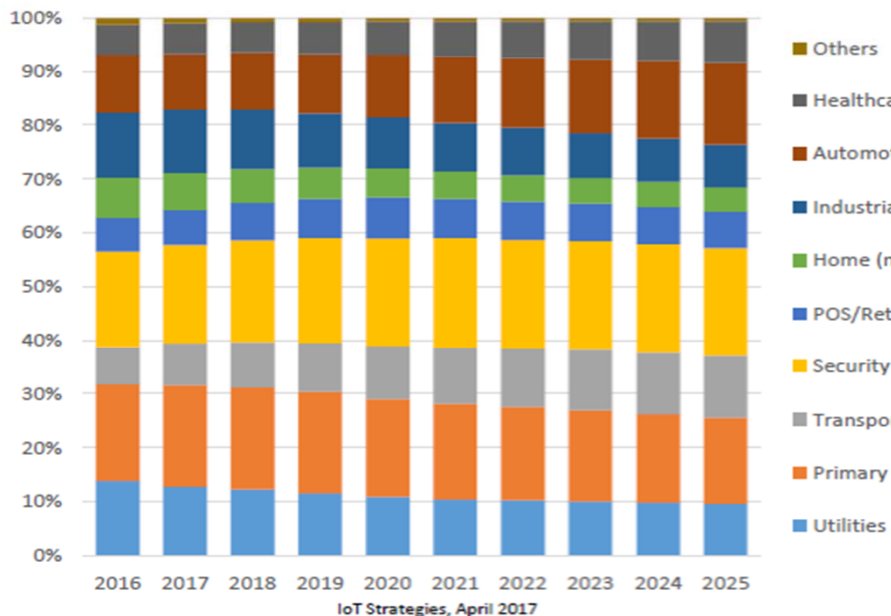
70% of IoT revenues across 2016-2025.

Security, Primary Processing, Automotive, Transport and Utilities.

3 Verticals will Generate +\$50Bn
2025

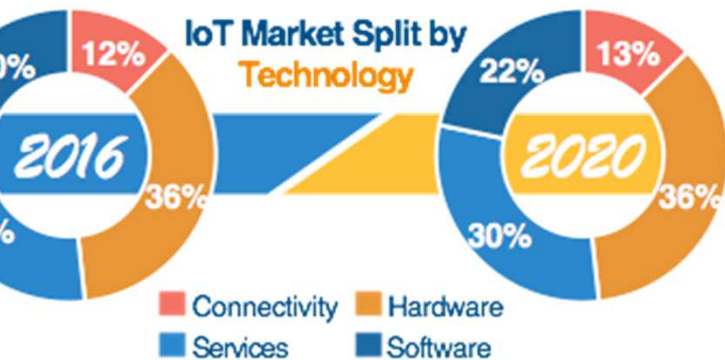
Security, Primary Processing and Automotive.

Total Annual IoT Revenues by Industry Vertical (%)



How the IoT European Market will Evolve across Techs, Verticals, and Use Cases

European IoT Market Forecast



THE LARGE

Freight Monitoring
Transport

Manuf. Operations
Manufacturing

Smart Grid (Electricity)
Utilities

THE FAST

Smart Buildings
Cross-Industries

Airport Facility
Automation
Transport

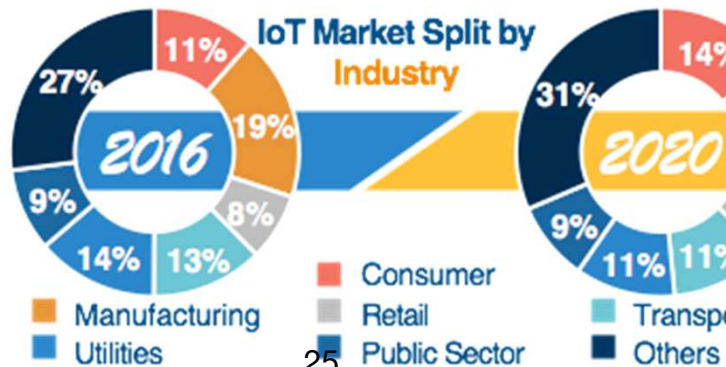
Connected Vehicles
Cross-Industries

WIDE UNEXPECTED

Vehicles as road
quality auditors

Phones as citizen
movement prediction

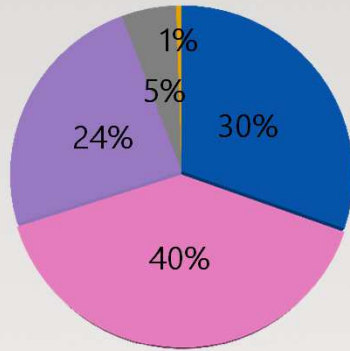
Snails as weather
Internet of Snail



European Industry Buyers' View

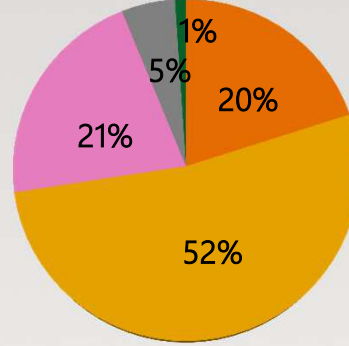
How important do you think the IoT could be to your organization (%)?

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important



What business impact do you think the IoT will have on your organization?

- Transformational
- Strategic
- Tactical
- For consideration
- Not impact at all to my organization



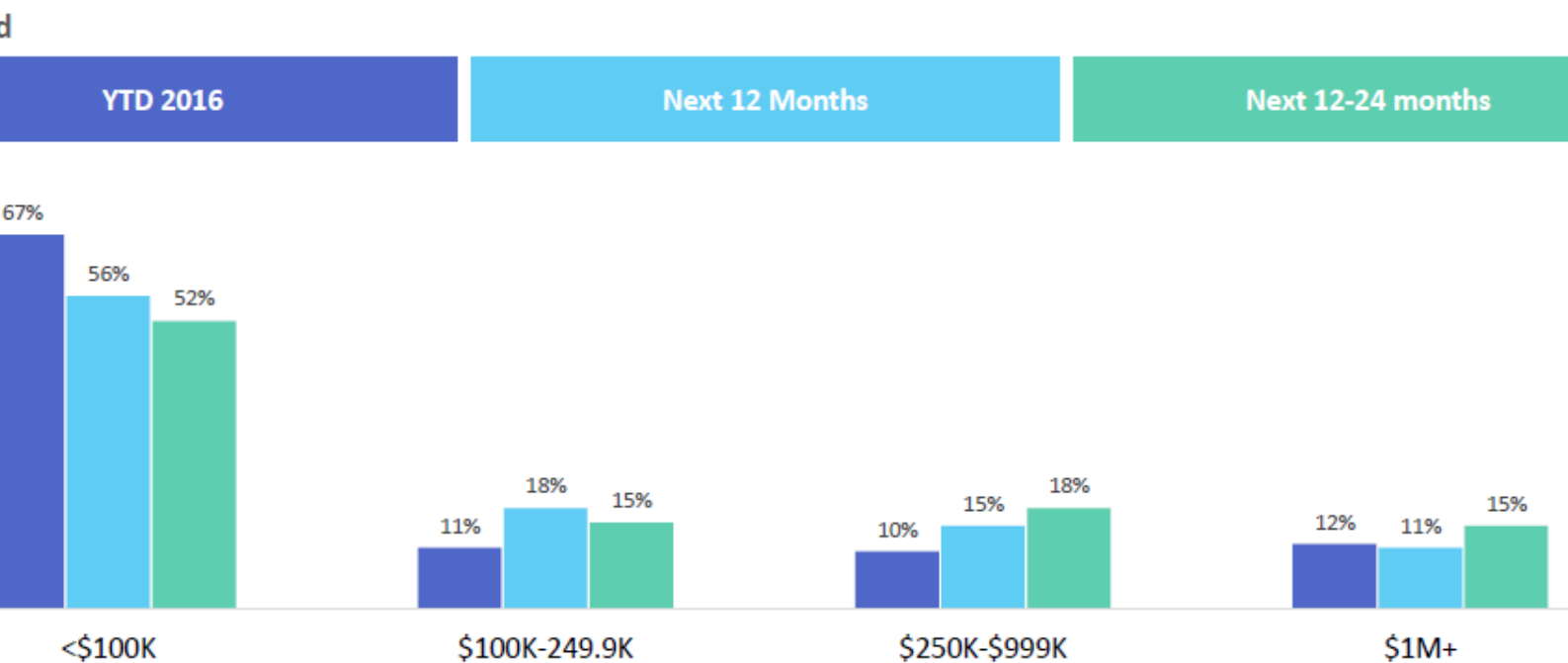
Drivers Behind Your IoT Strategy

1. Process automation
2. Improve business productivity
3. Improve customer experience
4. Reduce operational costs
5. Improve energy efficiency

Inhibitors to an IoT Solution Deployment

1. Security concerns
2. Upfront costs
3. Privacy concerns
4. Ongoing costs
5. Existing infrastructure limits

ing on IoT is expected to increase little by little over the next 2 years,
over half of Manufacturers will remain in the <\$100K bracket



4-Some challenges

Implementation Concerns



Change of paradigm

Enterely new security threats	Business model shift	Unprecedented data volume	New Privacy landscape	Many standards
<ul style="list-style-type: none">• Devices decentralized & distributed• Connected vehicles, power plants, factory under hacker area of operations	<ul style="list-style-type: none">• Recurring service revenues streams. Capex to Opex• Traditional manufacturing is becoming IT centric• IoT towards Internet of Services	<ul style="list-style-type: none">• Connected sensors and gateways will transmit TB of data• Demand for real time analysis and decision• Demand for AI	<ul style="list-style-type: none">• Millions of devices collecting data on people and environnement• Regulatory & Compliance burden	<ul style="list-style-type: none">• Multitude of standards implemented which raises the cost of IoT implementation• Discourage developers and innovators

What can I deliver really ?

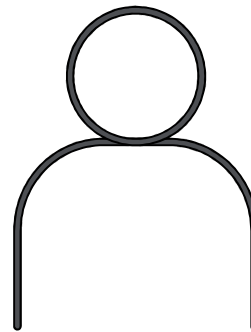
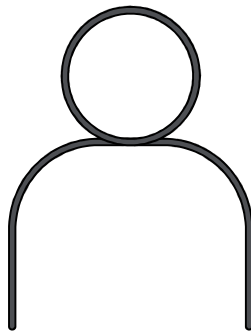
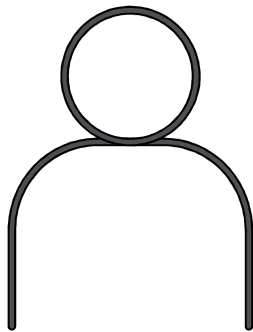
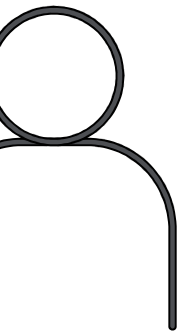
RELIABILITY
Can any device
connect to any app
any user, over any
network while
moving?

SECURITY
Are your IoT
communications
secured, data
access well
controlled, and
apps protected?

SCALABILITY
How many
assets, data,
apps, and users
can you support
safely?

VISIBILITY
Are you able to
understand and
track your devices
and the activity of
your networked
system efficiently?

PERFORMANCE
Is the user
experience
quality of service
ensured? Cost
and SLA
guaranteed?



Fast data
gestion

Contextual
awareness

Situational
awareness

Predictive
analytics

Prescriptive
analytics

data at speed
volume
000 events per
seconds

Correlate & enrich
with contextual data
to enable better decisions

Correlate with real
time situational data
contextual data affecting
smart grid equipment

Predict threat &
opportunities using
models generated by
machine learning

Trigger next best
actions using automa
rules & adaptive proces



Less than 1 sec ?

Some other figures/issues

Data

Data generated by IoT devices will account for 10% of the world data

In 2020 the IoT is expected to generate 1000x more data than in 2015

In 2020 the overall power consumption expected to be 25 PWh (Callewaert 2016)

IP addresses exhaustion

32 bit IP v4 suitable for only 4×10^9 addresses

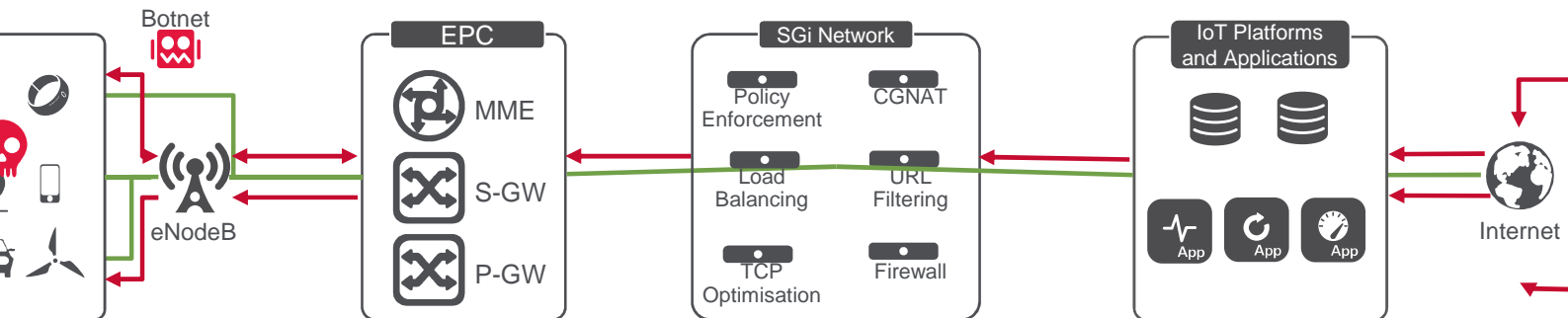
128 bit IP V6 suitable for 10^{38}

Internet protocol was not designed for real time

Mitigation by moving intelligence to concentrators and not in cloud

5-Security issues

Multi-Dimensional Threat Vectors to IoT Services



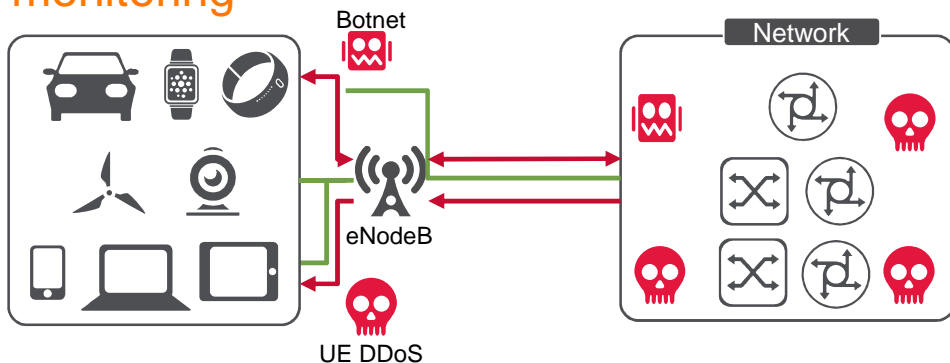
NETWORK DOMAIN			SERVICES DOMAIN
User Security	Network Security	Signaling Security	Application Security
<ul style="list-style-type: none"> Battery drain attacks File malware and bots Out-of-band security services 	<ul style="list-style-type: none"> RAN resource exhaustion Revenue leakage Terms and conditions violations 	<ul style="list-style-type: none"> Signaling overload/DDoS DNS security/DDoS Diameter firewall 	<ul style="list-style-type: none"> L7 DoS protection SSL offload IP intelligence and bot detection

IoT can be considered as a "new mobile service", it can leverage some of the above security techniques, plus it may require a few new ones

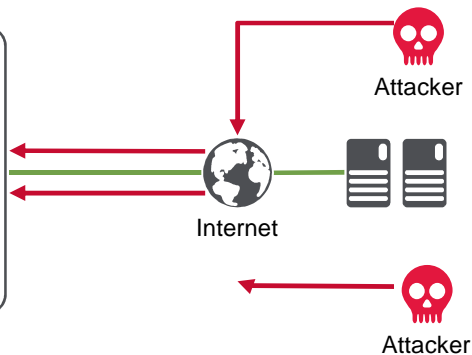
Internet of Things – Security in the Network Domain

Protecting the network infrastructure and the devices

Lack of device monitoring



New exploits can impact millions of devices



Proven security techniques for mobile broadband services (Gi Firewall, Anti-DDoS, IPS security, etc.) are very important for IoT applications

At the scale of deployment is much larger (bandwidth and connections per second)

Example of attacks from IoT but not only....

- 21st october 2016
 - Dyn is a DNS provider, meaning it helps direct domain names back to certain IP addresses for many major companies. During the attack, brands such as Twitter, Amazon, Reddit, Netflix, and more were without service multiple times during the day. (millions of IP addresses involved)
- 1st of Nov 2016
 - Liberia has been hit with one of the most harmful **DDoS** attacks yet, with most of its residents unable to get online. (>500 Gbps)
- 29th of Nov 2016
 - Hundreds of thousands of Deutsche Telekom customers in Germany had their broadband service cut off following a hack-attack on its hardware. (around 900K) but unsuccessful take over of the equipment by the hacker.

Security Fail Examples

network

application

mobile

cloud

IoT

- ◆ 10/10 security systems accept '1234'
- ◆ 10/10 security systems with no lockout
- ◆ 10/10 security systems with enumeration
- ◆ SSH listeners with root/"" access
- ◆ 6/10 web interfaces with XSS/SQLi
- ◆ 70% of devices not using encryption
- ◆ 8/10 collected personal information
- ◆ 9/10 had no two-factor options
- ◆ Unauthenticated video streaming
- ◆ *Completely flawed* software update s

Example 1 :DEFCON 2017 & the Voting Village



Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure

September 2017

Co-authored by:

Matt Blaze, University of Pennsylvania

Jake Braun, University of Chicago & Cambridge Global Advisors

Harri Hursti, Nordic Innovation Labs

Joseph Lorenzo Hall, Center for Democracy & Technology

Margaret MacAlpine, Nordic Innovation Labs

Jeff Moss, DEFCON

Lessons

- Lesson #1: Even with limited resources, time, and information, voting systems can be hacked.
 - The DEFCON Voting Village showed that technical minds with little or no previous knowledge about voting machines, without even being provided proper documentation or tools, can still learn how to hack the machines within tens of minutes or a few hours.
 - **AVS WinVote** : Carsten Schürmann, a democracy-tech researcher who hails from Denmark, was able to hack into the AVS WinVote within minutes remotely over Wi-Fi.
 - **AccuVote-TSx** :
 - **ES&S iVotronic** ;
 - **Sequoia AVC Edge** :it appeared that there may be use of an *8-bit cipher* (eight (8) bits is exceedingly insecure)
- Lesson #2: Foreign-made parts introduce serious supply chain concerns.

Example 2 : Pacemaker ecosystem evaluation

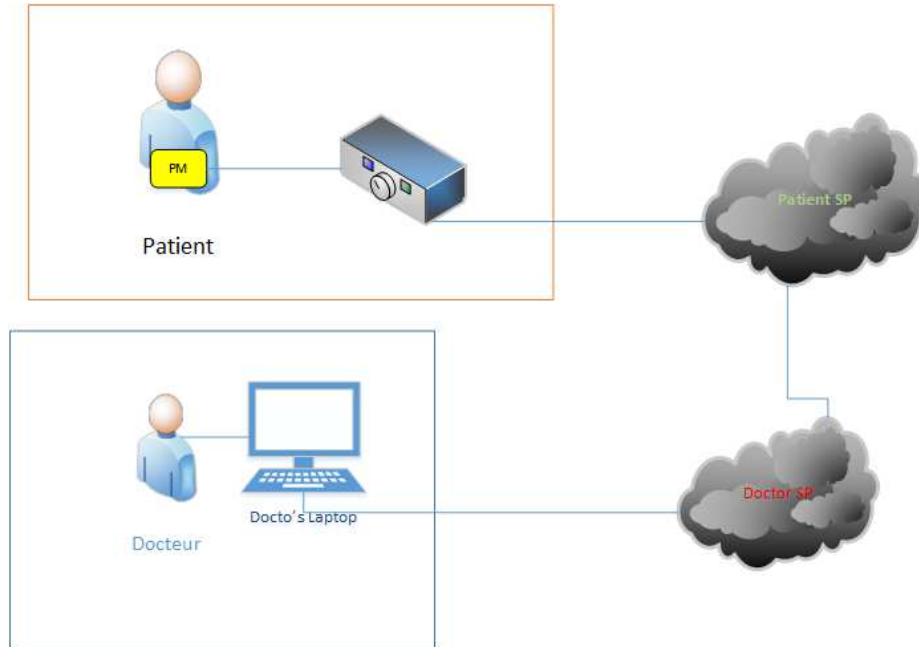


Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies

Billy Rios
Jonathan Butts, PhD

May 17, 2017

Architecture



Results

	Vendor 1	vendor 2	Vendor 3	Vendor 4	Mean
Nb of identified 3rd party components	201	47	77	21	87
Nb of vulnerable 3rd party components	74	39	41	10	41
Nb of known vulnerabilities identified in 3rd party components	2354	3715	1954	642	2 166

In average 50 vulnerabilities by component !

6-Privacy issues

me identified threats

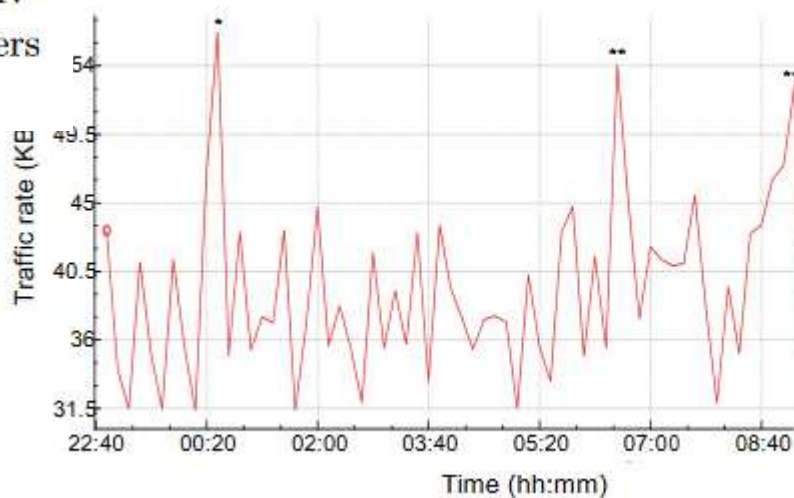
1. Passive listening of traffic
2. Illegitimate use of your data by your ISP or supplier of IoT
3. Data-mining of several anonymized pools of data

Passive listening

Noah Apthorpe*, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick

Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic

Privacy threat of traffic metadata analysis will continue to grow along with the market for IoT smart home devices. In this paper, we demonstrate that a passive network adversary can infer private in-home user activities from smart home traffic rates and packet headers even when devices use encryption.



Illegitimate use of your data by your ISP or supplier of IoT



TECHNOLOGY

Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data

by MIKE ISAAC and STEVE LOHR APRIL 24, 2017



Data-mining of anonymized pools of data

- Unfortunately we are only 7 billion human being ! 2^{33}
- Re-identification techniques are well developed through the use of passive or active meta data
- Privacy preserving data analysis has its own limits
 - See “*The Algorithm foundations of differential privacy*” by Cynthia Dwork & Aaron Roth.
- The digital traces left by human are huge
 - metadata and semantic allows a real re-identification of people or group of people

Just 2 examples !

US census

- Give your post code, sex and date of birth and I will have 63% chance to re-identify you uniquely
 - Uniqueness of simple demographics in the US population, L. Sweeney Carnegie Mellon University

Netflix

- If I got 8 comments from you on the films you have seen during the last 15 days, I can re-identify with 99% probability all the videos you have seen !
 - Robust De-Anonymization of Large Sparse datasets, Arvind Narayanan & Vitaly Shmatikov in PROC OF the 2008 IEEE SYMP. ON SECURITY AND PRIVACY

<https://panopticlick.eff.org/results?#fingerprintTable>

Your browser fingerprint **appears to be unique** among the 779,156 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 19.57 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

AUG 31, 2017 @ 05:18 PM 817

The Little Black Book

If Consumer Privacy Isn't Already Dead, IoT Could Kill It



Nikki Baird, CONTRIBUTOR

I focus on the digital consumer's impact on retail. [FULL BIO](#) ✓

Opinions expressed by Forbes Contributors are their own.

ain take aways

The growth of IoT devices bring new challenges for the industry

- business model & profitability (where is the break even point ?)

The average user will be part for at least 1 botnet network if he has more than 10 IoT...

The industry has to carefully design their inclusion in the production line and invest massively in **permanent monitoring** of theses infrastructures.

For the global consumer, **IoT could be the killer of privacy** without strong regulation:

1. Education has to take into account the negative impact of digital services on privacy.
2. Democracy is based on strong respect of privacy with capacity to verify the use made by private & public sector
 1. Independent agencies required

As always the positive and negative effects will fluctuate, hope the good side will win the race. Europe has good chance to pave the way for a balanced approach.

Thank you for your attention

