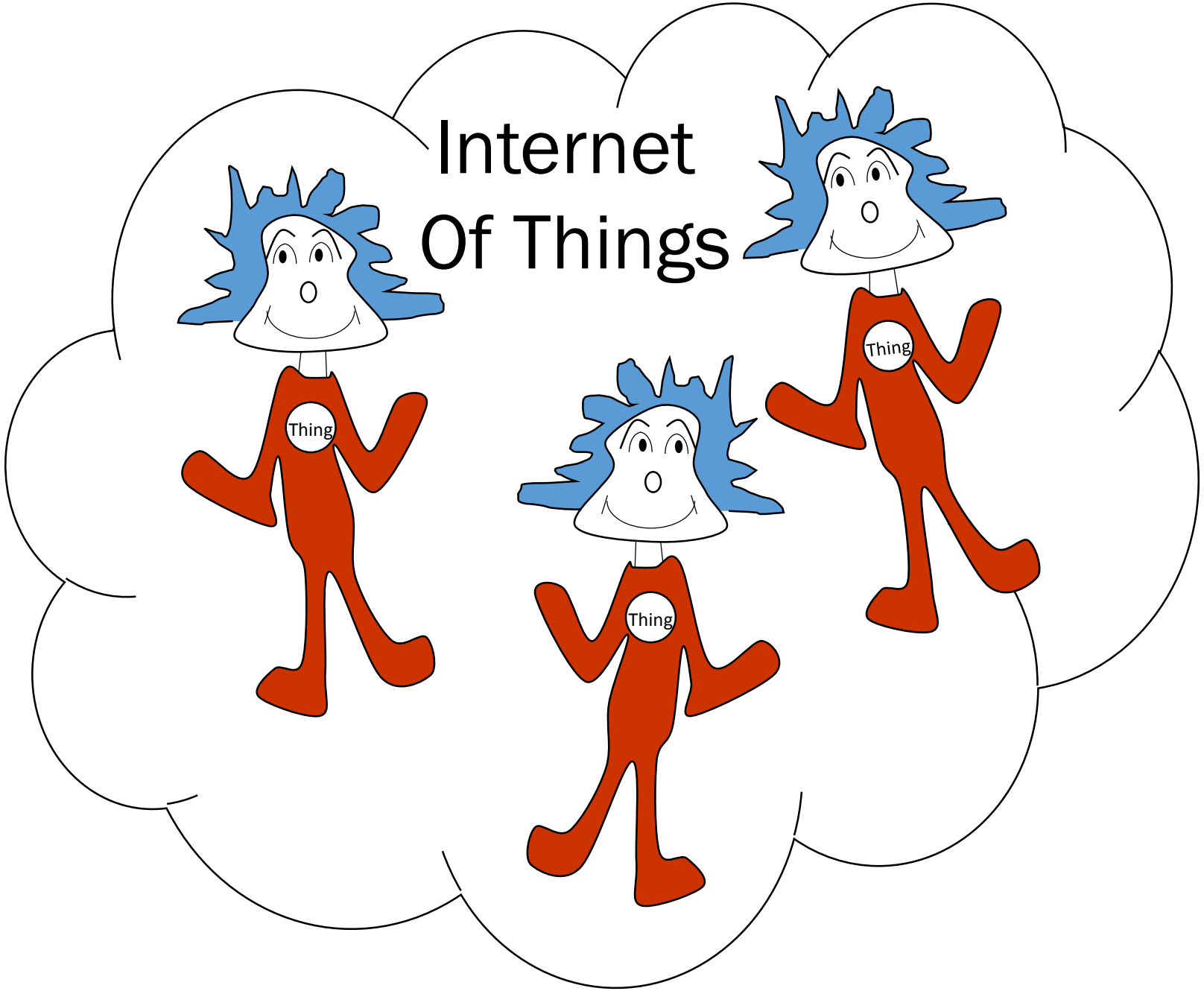
LA-UR-15-23789
Approved for public release; distribution is unlimited.

Title: Internet of Things

Author(s): Frost, Sandra L.

Intended for: DOE Control System Security, 2015-05-07 (Los Alamos, New Mexico, United States)

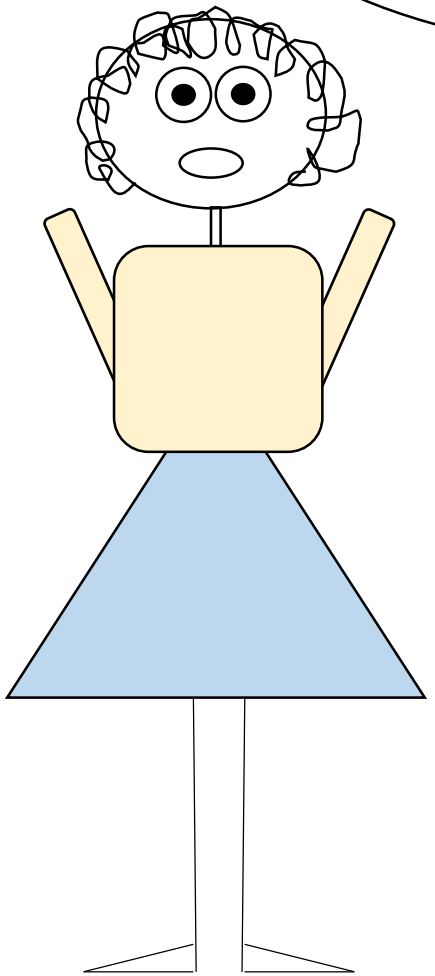
Issued: 2015-05-20

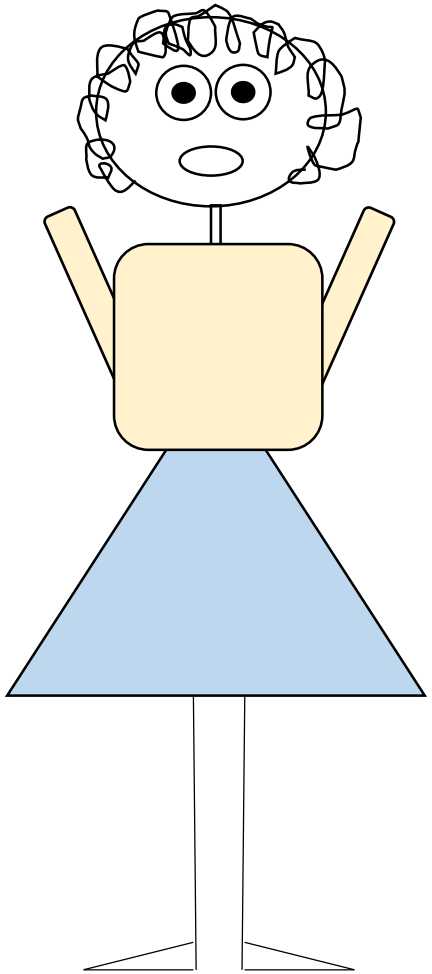


Sandy Frost/LANL

http://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

But really, what is the “Internet of Things”?





It’s not that easy….

‘Things’ in the Internet of Things: Towards a Definition

Edewede Oriwoh*, Marc Conrad

Computer Science and Technology Department, University of Bedfordshire, Bedfordshire, LU1 3JU, United Kingdom

Abstract This work is an attempt to provide a definition of the word ‘Things’ in the context of the Internet of Things (IoT). It does this partly by reviewing the existing descriptions of, and variations to, the IoT phrase as well as the alternative terms that have so far been used to replace the word ‘Things’ in the phrase. This review was done to draw from these different terms and descriptions a sense of the wide breadth of the examples of ways that ‘Things’ in the IoT can manifest. An attempt is made to relate all the relevant but varied definitions and descriptions in order to draw up a definitive definition which can serve as a reference for stakeholders who are keen to understand the IoT concept as it exists presently as well as in the future.

Keywords Internet of Things, Things, Definition

1. Introduction

Ever since the phrase ‘Internet of Things (IoT)’ was coined in 1999 [1], it has been attributed a variety of descriptions; it has been described as a network [2], a paradigm [3, 4], a concept [5], an Internet application [6] and a global network infrastructure [7], to mention a few. In addition, the word ‘Things’ in the IoT phrase has been replaced with several alternative terms giving rise to several ‘Internets of α’ including the Internet of Everything (IoE) [8, 9], Internet of Anything [10], Internet of People [11, 12], and the Internet of Signs [13, 14] among other examples.

The first word in the IoT phrase, ‘Internet’, has already be noted, is not necessarily limited to the Internet previously described).

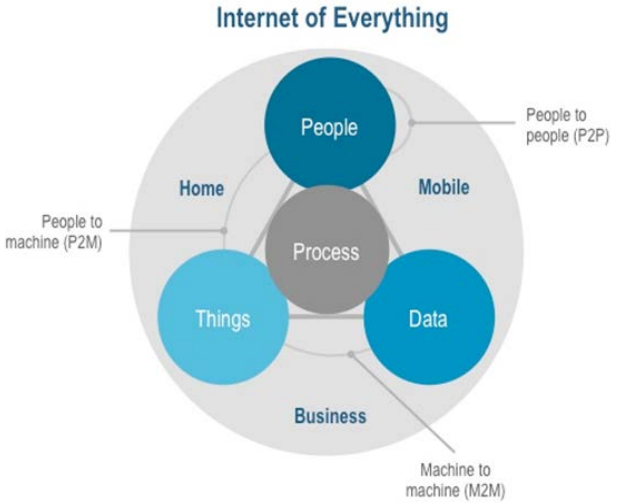
Next is the word *Things* and deriving a unified description for this word forms the bulk of the discussion in this paper. Gubbi explains that “the definition of ‘Things’ has changed as technology evolved” [2]. Stakeholders within the IoT context have created - or are creating - their own understanding of what ‘Things’ are and what the word can represent. What this paper proposes is a definition of ‘Things’ so that anyone approaching the subject of the IoT can quickly grasp what it means and what it can mean for various stakeholders going forward. The aim of defining ‘Things’ in this paper is not to restrict the concept of the IoT to mean the interconnection of only a select type of

article.sapub.org/10.5923.j.ijit.20150401.01.html

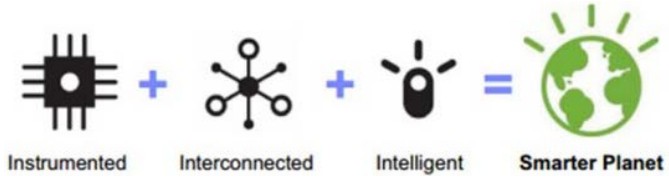
Multiple Definitions

Industrial Internet
A term coined by *General Electric* and refers to the integration of complex physical machinery with networked sensors and software.

Cisco



IBM



NIST Cyber-Physical Systems
Smart systems that include co-engineered interacting networks of physical and computational components

Wikipedia
The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

Microsoft

Creating the Internet of Your Things

Google
A proposed development of the Internet in which every day objects have network connectivity, allowing them to send and receive data

FTC
Although the term “Internet of Things” first appeared in the literature in 2005, there is still no widely accepted definition.

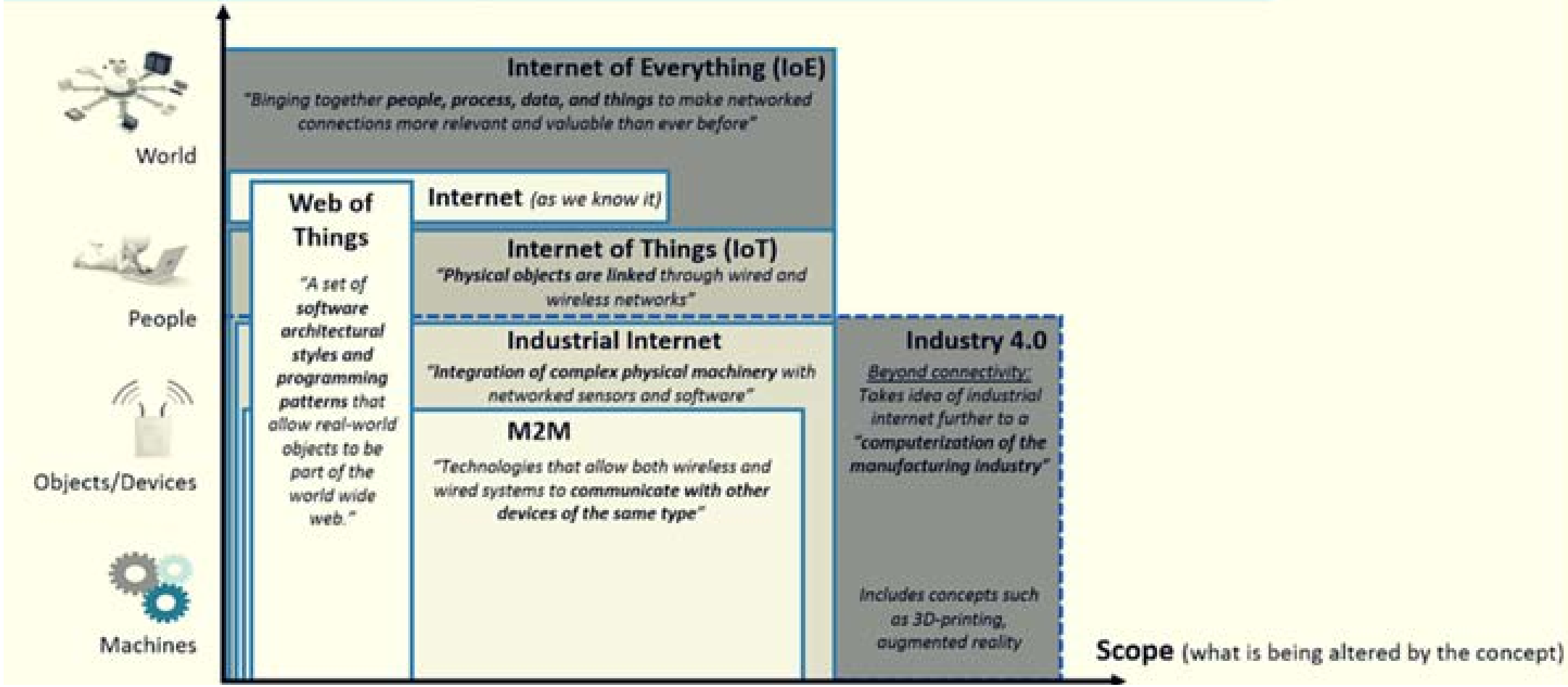
Gartner
Network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

Oxford - 2013
The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

http://blogs.cisco.com/ioe/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic, http://ibmcai.com/2014/07/23/building-a-smarter-planet-through-an-intelligent-internet-of-things, http://embedded-things.blogspot.com/2015/02/creating-internet-of-your-things.html, https://www.rti.com/

Why the Internet of Things is called Internet of Things?

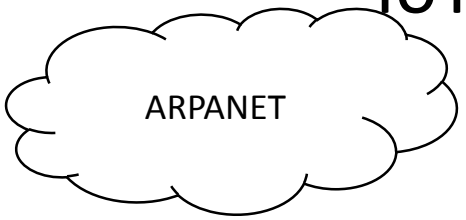
Definition, history, disambiguation



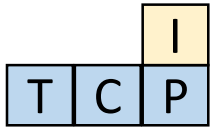
http://iot-analytics.com/internet-of-things-definition/

IoT History

1946



1969

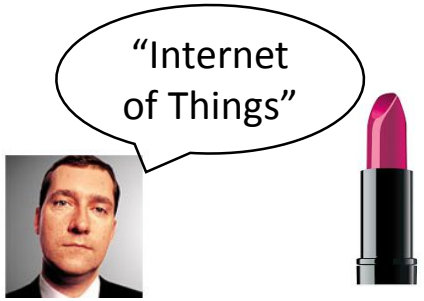


1982


John Romkey, 1st Internet device

1990

1998



Kevin Ashton coined the term IoT

2000

http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, https://learn.sparkfun.com/tutorials/bluetooth-basics, http://www.rfidjournal.com/articles/view?4986, courseimage.com

Jun 22, 2009

The fact that I was probably the first person to say "Internet of Things" doesn't give me any right to control how others use the phrase. But what I meant, and still mean, is this: Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture or scanning a bar code. Conventional diagrams of the Internet include servers and routers and so on, but they leave out the most numerous and important routers of all: people. The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world.

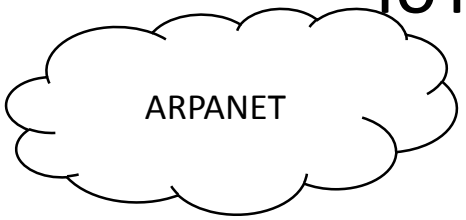
And that's a big deal. We're physical, and so is our environment. Our economy, society and survival aren't based on ideas or information —they're based on things. You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things.

If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best.

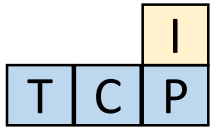
http://www.rfidjournal.com/articles/view?4986

IoT History

1946



1969

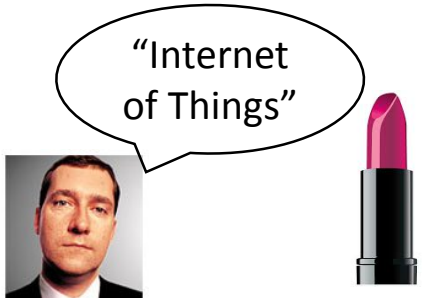


1982

John Romkey, 1st Internet device

1990

1998

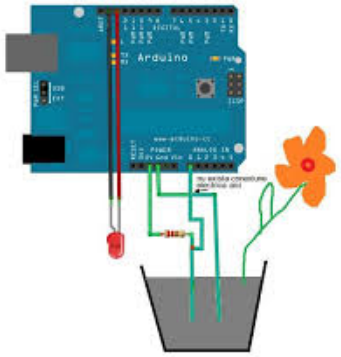


Kevin Ashton coined the term IoT

2000

LG's 1st Internet Fridge ($20K)

2005



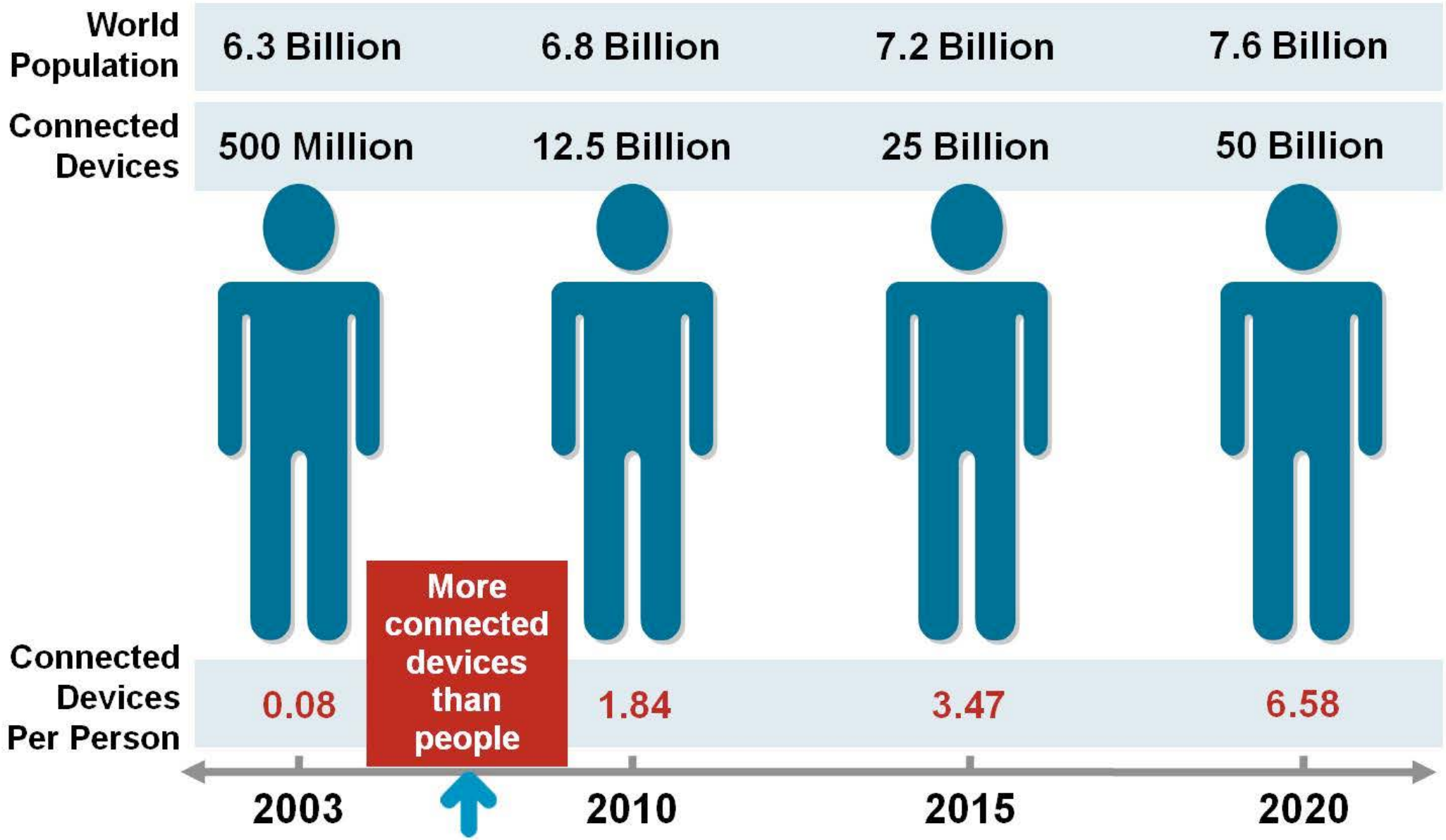
2008

Cisco said IoT was born, since more things than people on Internet

2008-9

http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, https://learn.sparkfun.com/tutorials/bluetooth-basics, http://www.rfidjournal.com/articles/view?4986, courseimage.com, http://www.electroschematics.com/6519/simple-soil-moisture-sensor-arduino-project/, http://pixshark.com/stork-flying-drawing.htm

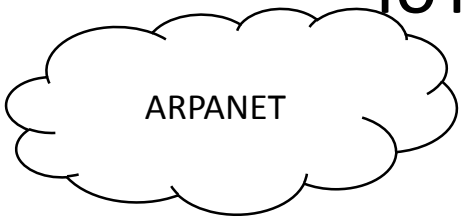
The Internet of Things was “Born” Between 2008 and 2009



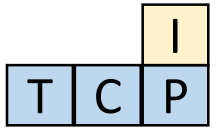
http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

IoT History

1946



1969

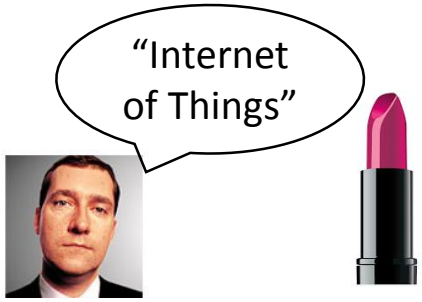


1982

John Romkey, 1st Internet device

1990

1998

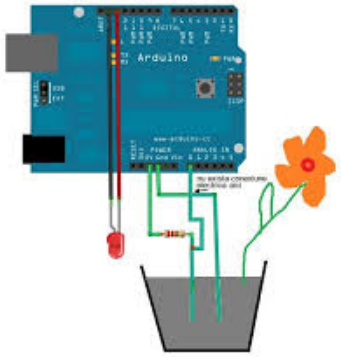


Kevin Ashton coined the term IoT

2000

LG's 1st Internet Fridge ($20K)

2005

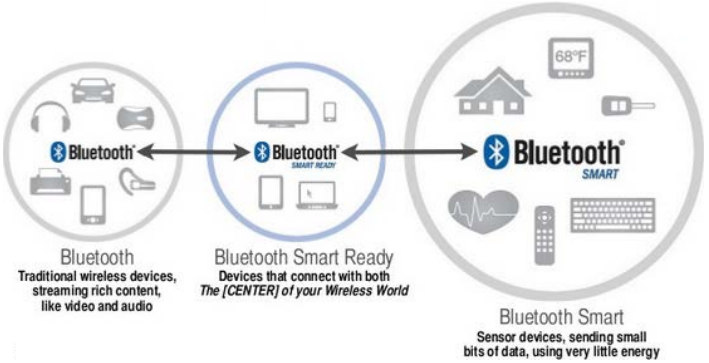


2008

Cisco said IoT was born, since more things than people on Internet

2008-9

2010



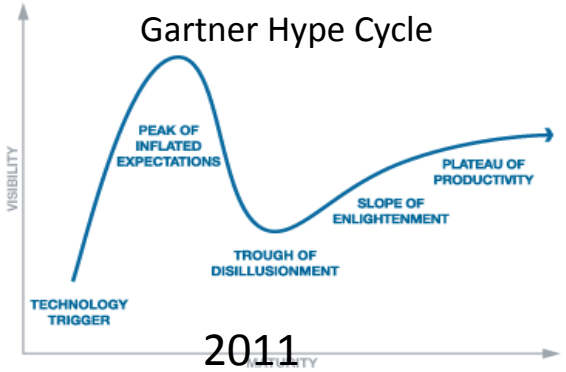
2011

2011

http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/, https://learn.sparkfun.com/tutorials/bluetooth-basics, http://www.rfidjournal.com/articles/view?4986, courseimage.com, http://www.electroschematics.com/6519/simple-soil-moisture-sensor-arduino-project/, http://pixshark.com/stork-flying-drawing.htm,powerelectronics.com, www.edn.com, http://www.worldipv6launch.org

IoT History

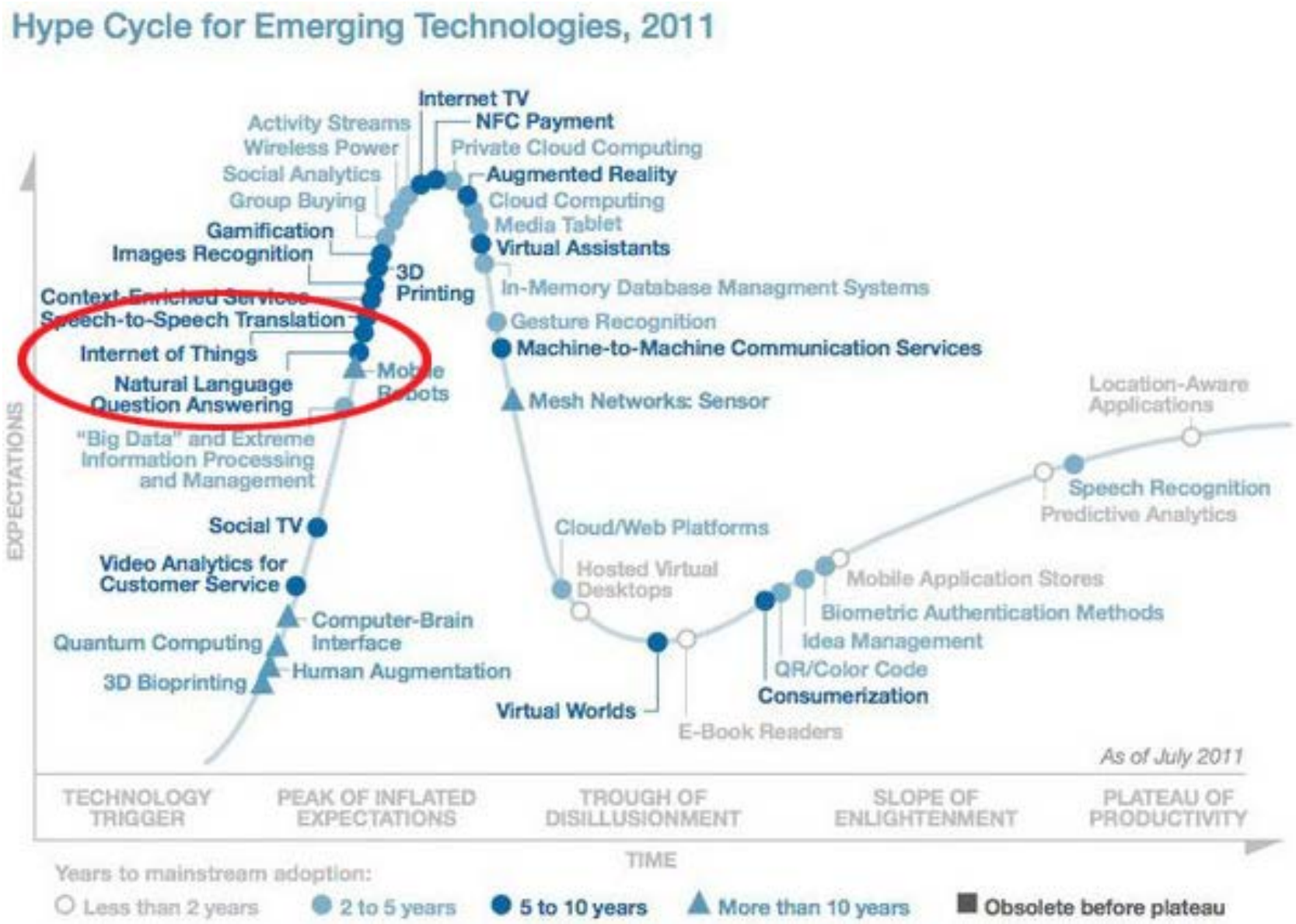
Gartner Hype Cycle



2011

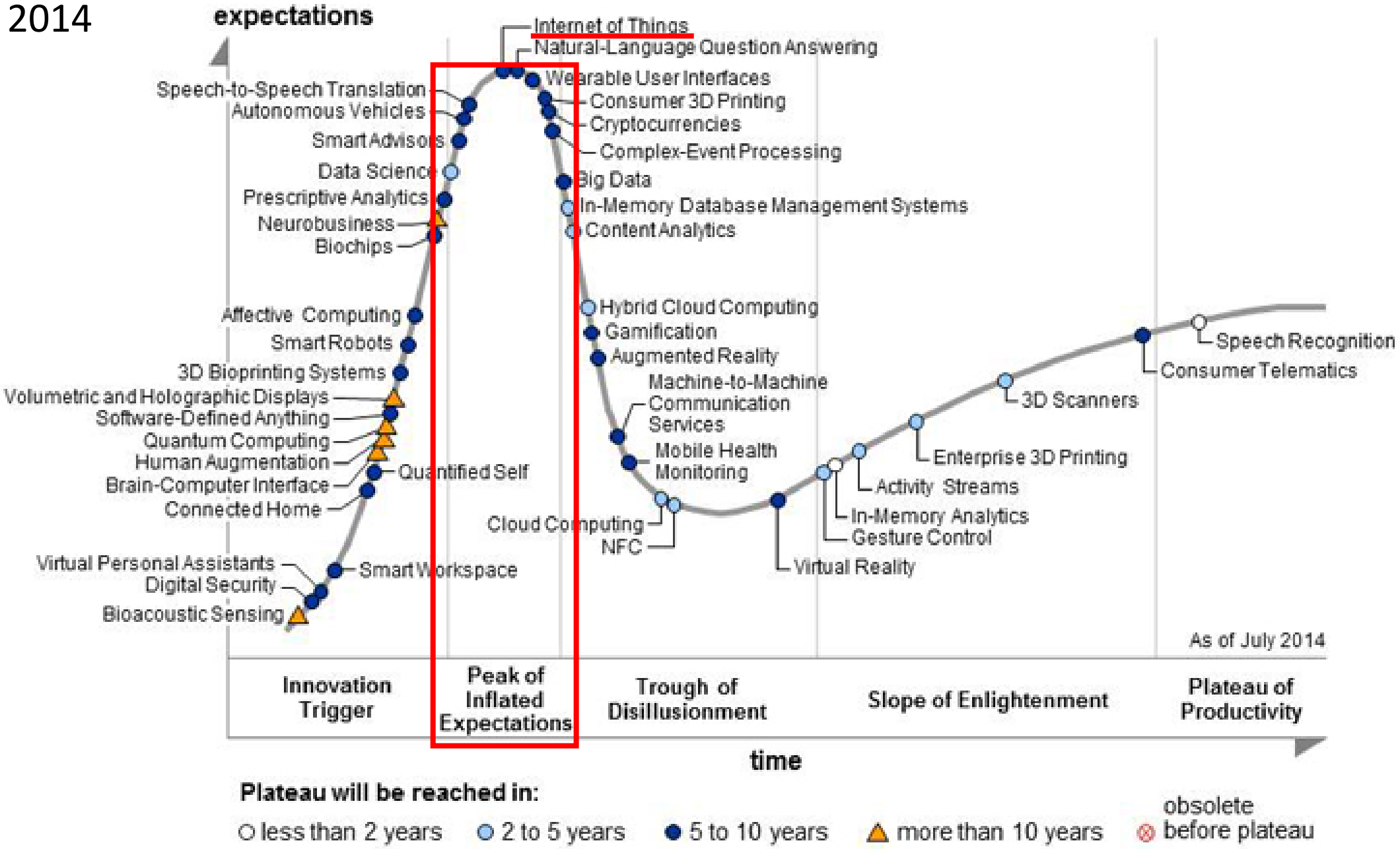
http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

July 2011



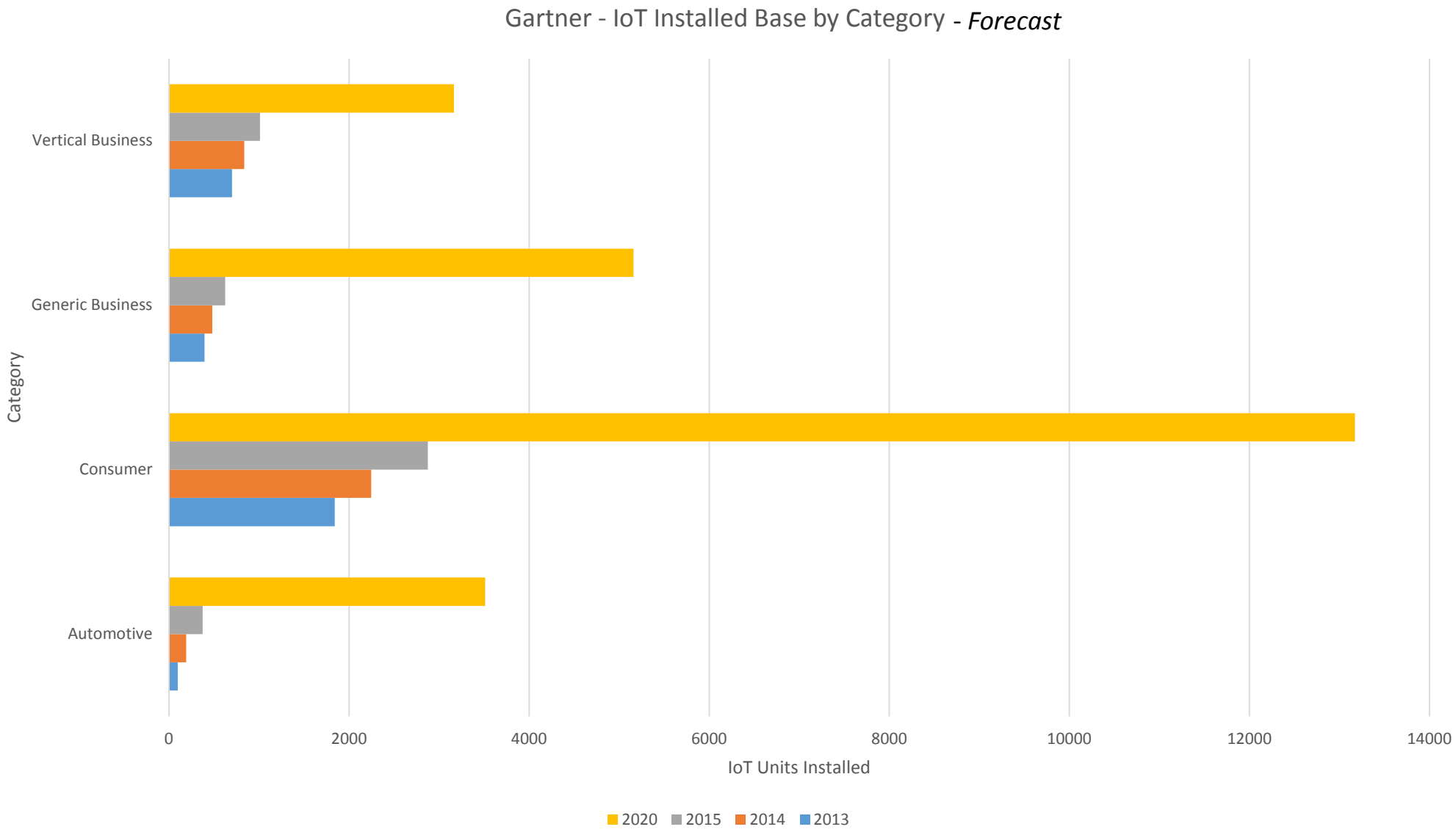
http://postscapes.com/internet-of-things-history

July 2014



http://postscapes.com/internet-of-things-history

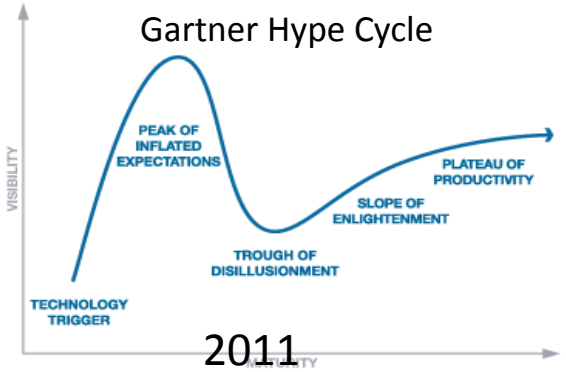
Nov. 11, 2014



http://www.gartner.com/newsroom/id/2905717

IoT History

Gartner Hype Cycle



2011

2011

2013

Venture Beat named 2014

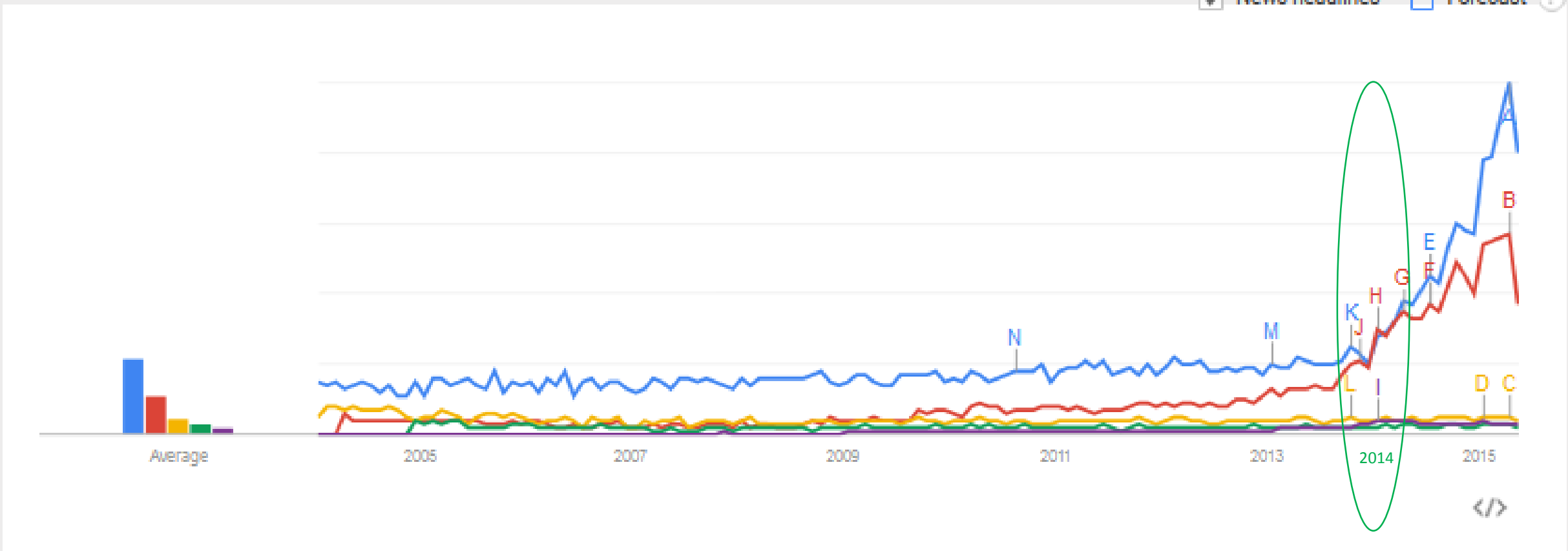
as the "Year of the Internet of Things."

2014

http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp, https://nest.com/thermostat/life-with-nest-thermostat/, blog.atmel.com, http://blog.atmel.com/2015/04/09/a-look-back-at-the-history-of-the-internet-of-things/

iot	Internet of things	industrial internet	Web of things	Internet of everything
Search term	internet o... Search term	industrial... Search term	web of th... Search term	internet o... Search term

Interest over time



http://www.google.com/trends/explore#q=internet%20of%20things%2C%20iot&cmpt=q&tz=

Regional interest

iot | internet of things | industrial internet | web of things | internet of everythi...

Region | City

South Korea	100
Vietnam	53
Taiwan	46
Brazil	31
India	28
Japan	24
Singapore	23

▸ View change over time

Regional interest

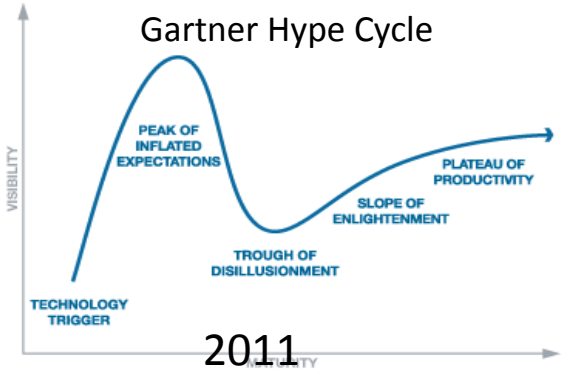
iot | internet of things | industrial internet | web of things | internet of everythi...

Region | City

Joinville	(Brazil)	100
Chiyoda	(Japan)	67
Blumenau	(Brazil)	45
Seoul	(S. Korea)	24
Fresno	(CA, US)	21
Florianópolis	(Brazil)	20
Florence	(Italy)	18

http://www.google.com/trends/explore#q=internet%20of%20things%2C%20iot&cmpt=q&tz=

IoT History



2011

2011

2013

Venture Beat named 2014 as the "Year of the Internet of Things."

2014

HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack

2014

BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES

Executive Office of the President

MAY 2014

2014

Google + nest

2014

Apple

HealthKit HomeKit

Microsoft

Health Intelligence Engine, HealthVault

2014

5 Industry Groups & Standards were launched in 2014 and one late in 2013

2014

Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015

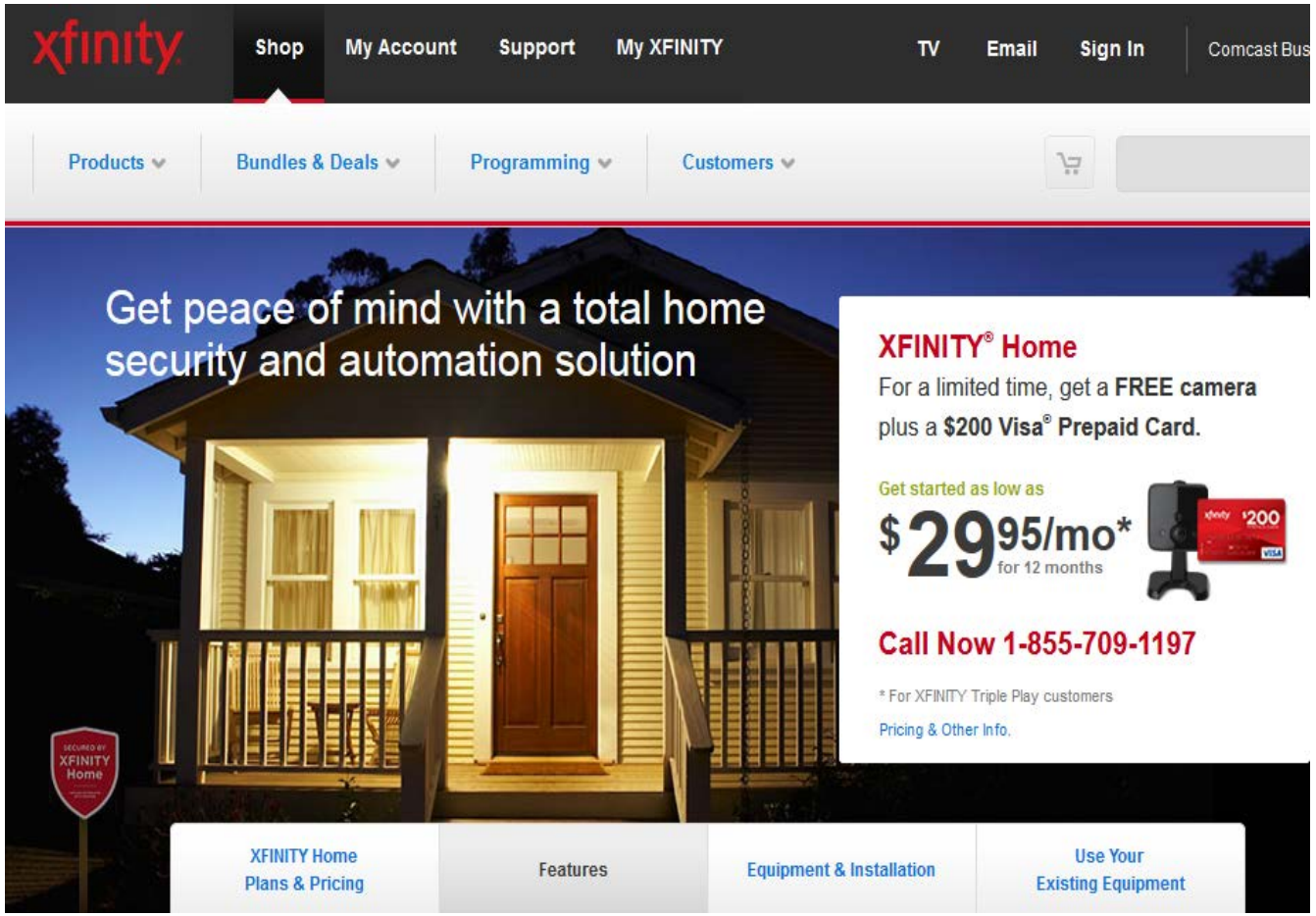
2015

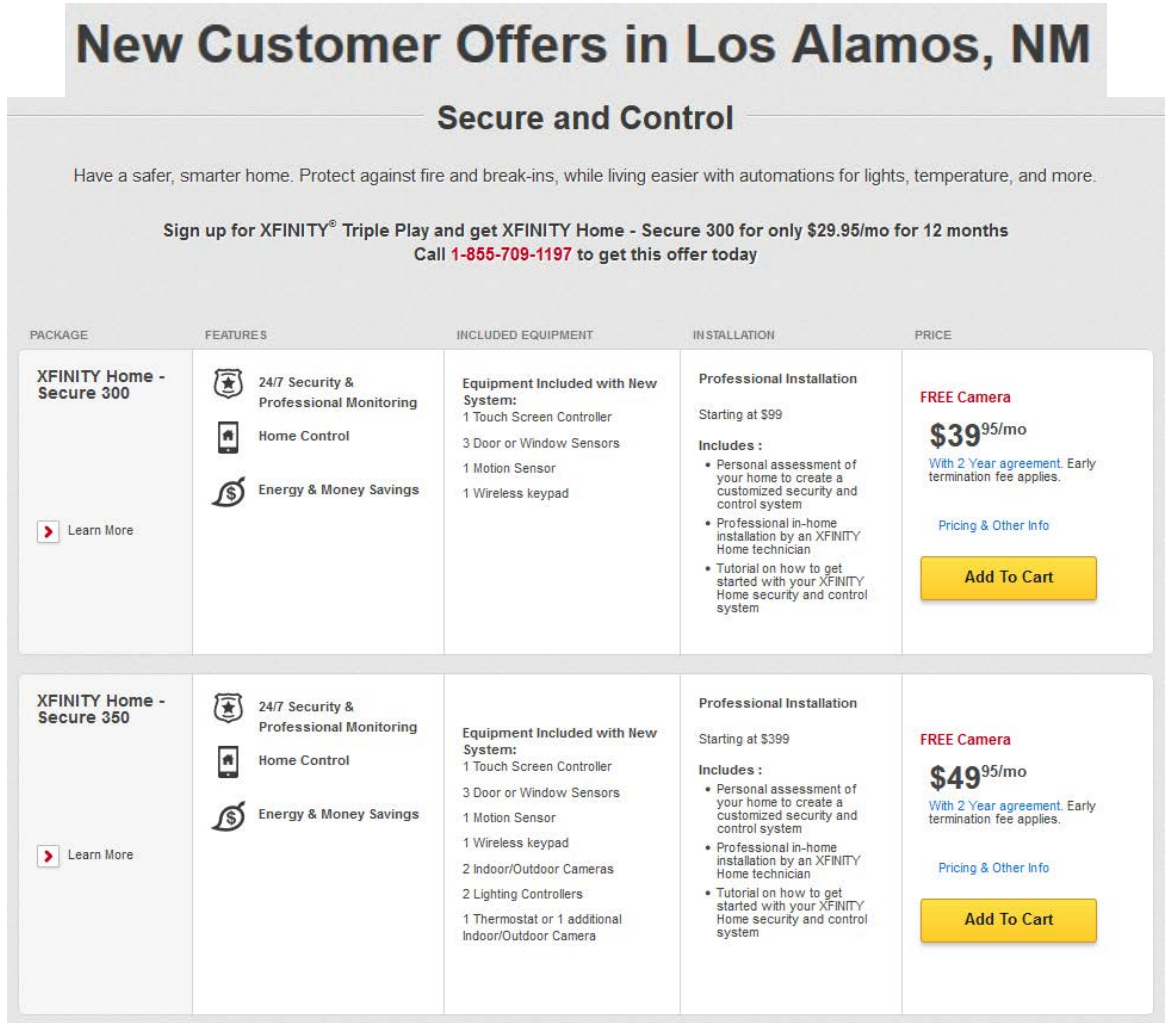
Comcast's Xfinity home platform adds Nest, August, and more

2015

http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VUKX-BDz2WE, http://www.eweek.com/networking/slideshows/a-look-back-at-internet-of-things-origin-evolution.html, nest.com, www.redmondpie.com, blogs.microsoft.com, http://www.gartner.com/newsroom/id/2905717, http://fortune.com/2015/05/05/comcast-xfinity-home/?xid=timehp-category

Comcast opened up its Xfinity Home platform to devices from some great startups such as Nest, August Locks, Rachio connected sprinklers, Skybell, Lutron and more. It was so exciting I sang a little ditty about the smart home going mainstream! IoT Podcast 5/6/15 (Stacey Higginbotham)





http://www.comcast.com/home-security/pricing.htm, http://iotpodcast.com/ I

Overview

- Definition
- Standards
- Studies, Surveys
- Security and Privacy
- Summary

Handbook: Internet of Things Alliances and Consortia

http://postscapes.com/internet-of-things-alliances-roundup

Handbook: Internet of Things Alliances and Consortia

http://postscapes.com/internet-of-things-alliances-roundup

Group	Founded	# of Members	Goal	Founding Members
Open Interconnect Consortium (Multilayer)	2014	62	Define and promote open source standards and implementation to improve interoperability across vertical markets and use cases	Atmel, Broadcom (no longer a member), Dell, Intel, Samsung, Wind River
AllSeen Alliance (Multilayer)	2011	133	AllSeen's AllJoyn open source project is a universal framework promoting interoperable products that can connect with all types of devices, systems, and services.	Haier, LG Electronics, Panasonic, Qualcomm, Sharp, Silicon Image, Sony, TP-Link, and others.
Thread Group (Vertical)	2014	97	Founded "to create the very best way to connect and control products in the home."	ARM, Freescale Semiconductor, Nest, Samsung, Silicon Labs, and others.
Industrial Internet Consortium (Vertical)	2014	148	Founded to "identify the requirements for open interoperability standards and define common architectures", case studies, and standard requirements.	AT&T, Cisco, GE, IBM, Intel
IPSO Alliance	2008	44	This Alliance promotes IP as solution for Smart Objects by documenting the use of IP-based technologies defined at the standard organizations like IETF.	Atmel, Cisco, Dust Networks, Emerson Climate Technologies, Freescale Semiconductor, SAP, Sensinode Oy, SICS, Silver Spring Networks, Sun Microsystems, and others.
Intel IoT Solutions Alliance *(formerly Intel Intelligent Systems Alliance)*	2011	250+	The Intel IoT Solutions Alliance "seeks to build a strong and sustainable market advantage through" solutions based on Intel architecture. "We work to drive revenue growth and market share for our members."	Intel **Premier (Non-founding) members:** ADLINK, Advantech, Dell OEM, Kontron, Portwell
Alliance for Internet of Things Innovation	2015	20+	Hoping to being together different industries, sectors, and companies in Europe, the AIOTI builds "on ongoing Commission initiatives to … foster European IoT innovation ecosystems."	Bosch, Philips, Sigfox, EU Commision

Source: VDC Research, 2015

Intel-led project

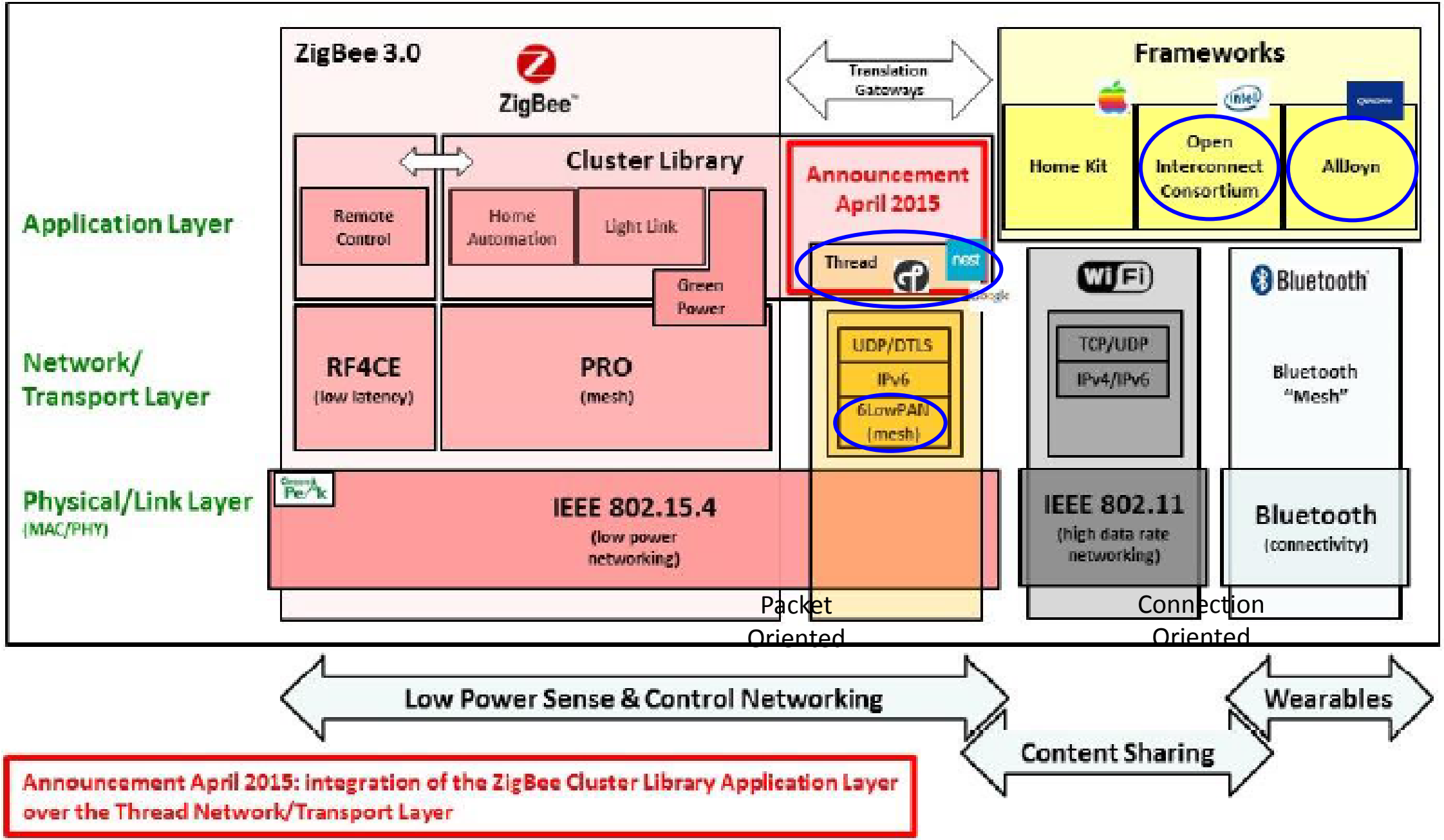
Competition
Linux Foundation
Discovery, connectivity

Qualcomm-led project

Google-led project
New Ip-based wireless networking protocol (mesh networking, 6LoWPAN

Intel-led project
Industrial Automation

http://blog.vdcresearch.com/embedded_hw/film/



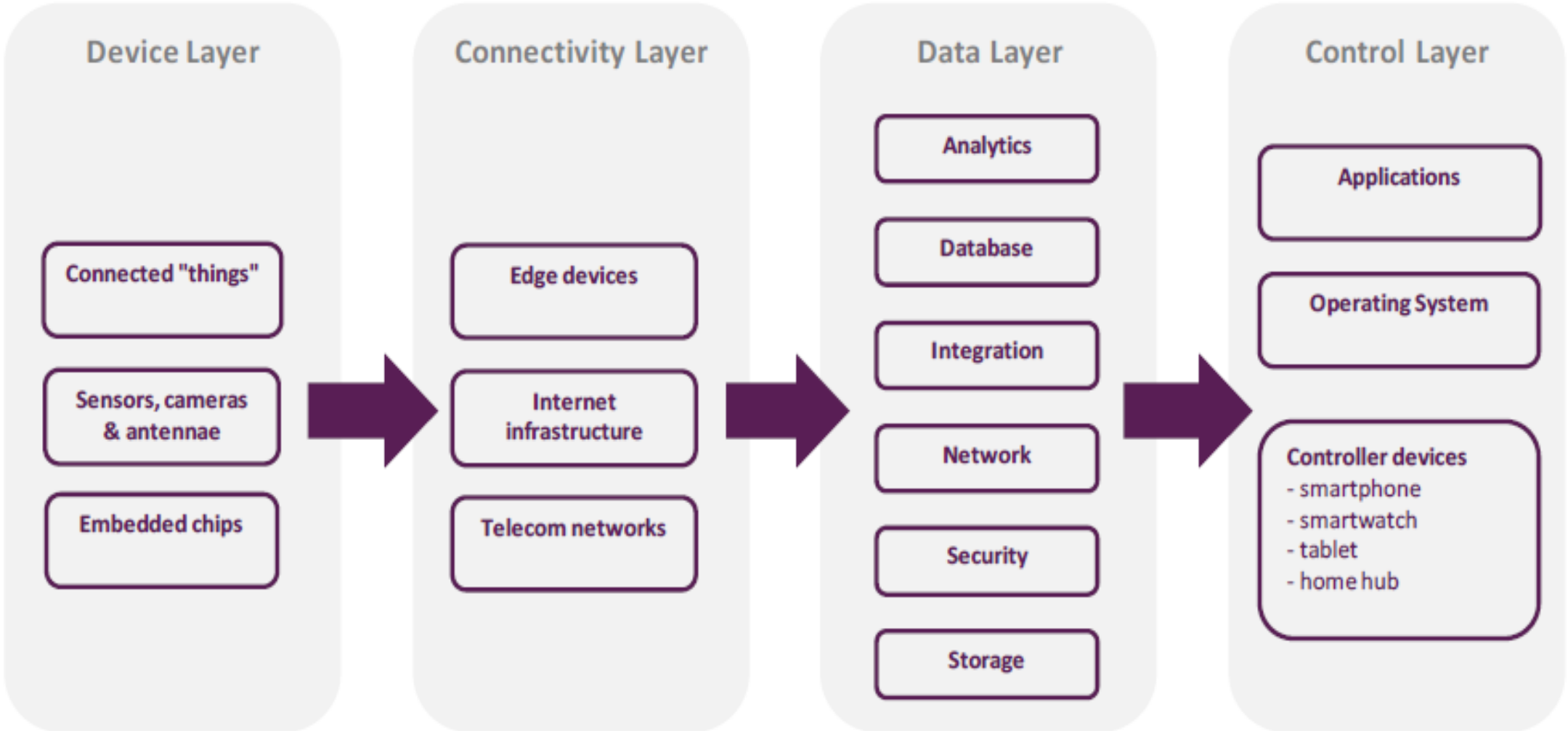
http://www.greenpeak.com/Press/PressKit/2015GreenPeakWhitePaperIoT&CommStandards.pdf

Overview

- Definition
- Standards
- Studies, Surveys
- Security and Privacy
- Summary

Value Chain

- We split the value chain for the Internet of Things into four layers: devices, connectivity, data and control.



http://www.slideshare.net/cmewawalla/the-internet-of-things-industry-trends-and-key-players

Key Players

Devices

Connected things	Philips Electronics LG Electronics Pace Panasonic Pioneer Samsung Electronics Sony
Sensors, microcontrollers & embedded chips	ARM Atmel Freescale Semi Infineon Intel InvenSense MediaTek Microchip Tech Micronas Semiconductor Nvidia Qualcomm Renesas STMicroelectronics Texas Instruments

Connectivity

Edge devices	Alcatel Lucent Cisco Ericsson Juniper Networks Nokia Sonus Networks
Internet / Cloud Infrastructure	21 Vianet Akamai Amazon F5 Networks Google Infoblox Rackspace Hosting
Telecom operators	AT&T BT China Mobile China Telecom Deutsche Telekom Level 3 NTT Softbank Telefonica Verizon Vodafone

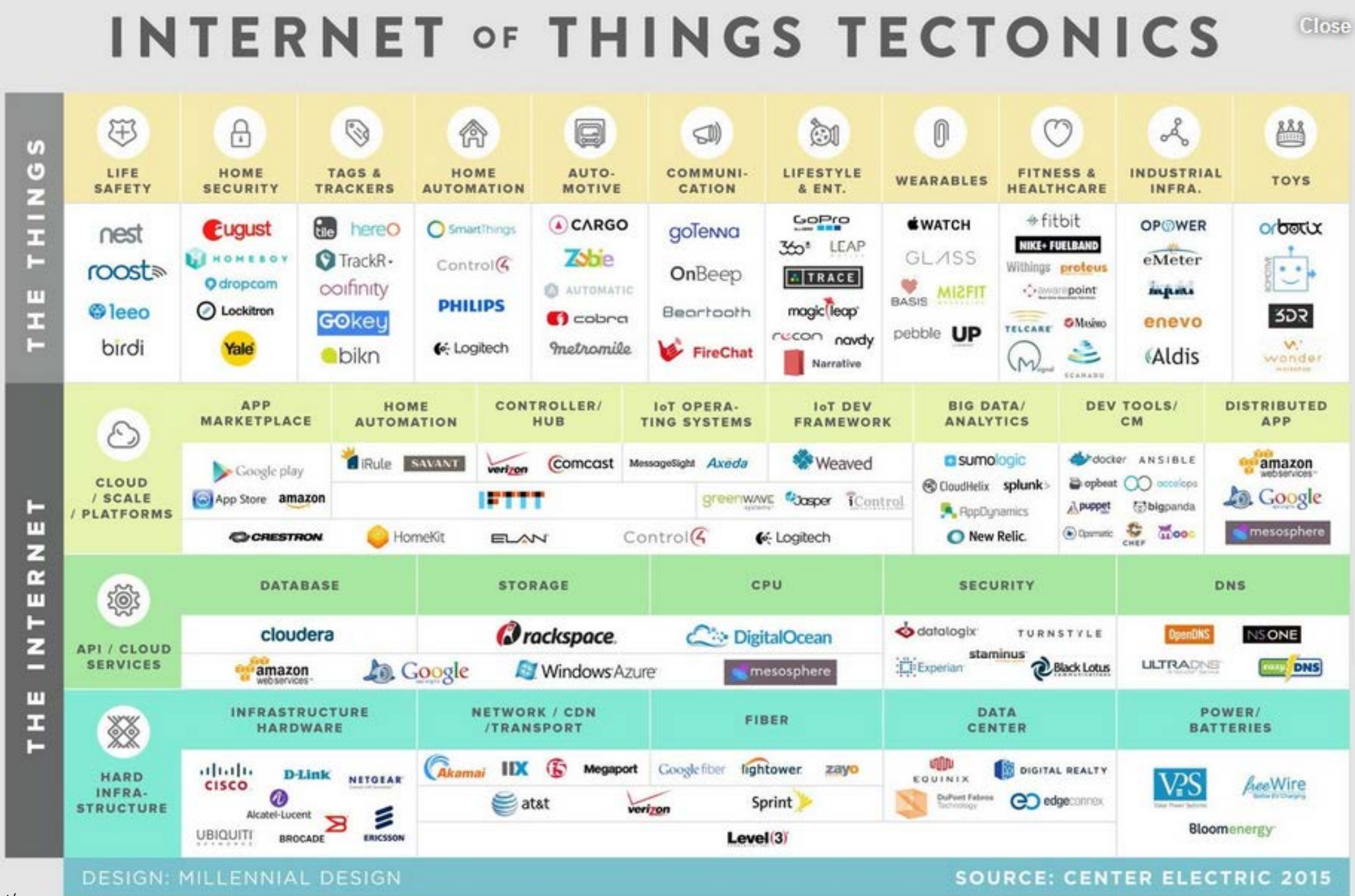
Data

Analytics	Qlik Tech Salesforce.Com Splunk Tableau
Database	IBM Oracle SAP
Integration	Citrix Systems Informatica Mobile Iron Red Hat VMware
Network	Arris Aruba Networks Brocade Comms Riverbed Tech ZTE
Security	Check Point Software FireEye Fortinet Palo Alto Networks Trend Micro
Storage	CommVault EMC Hewlett-Packard NetApp QLogic

Control

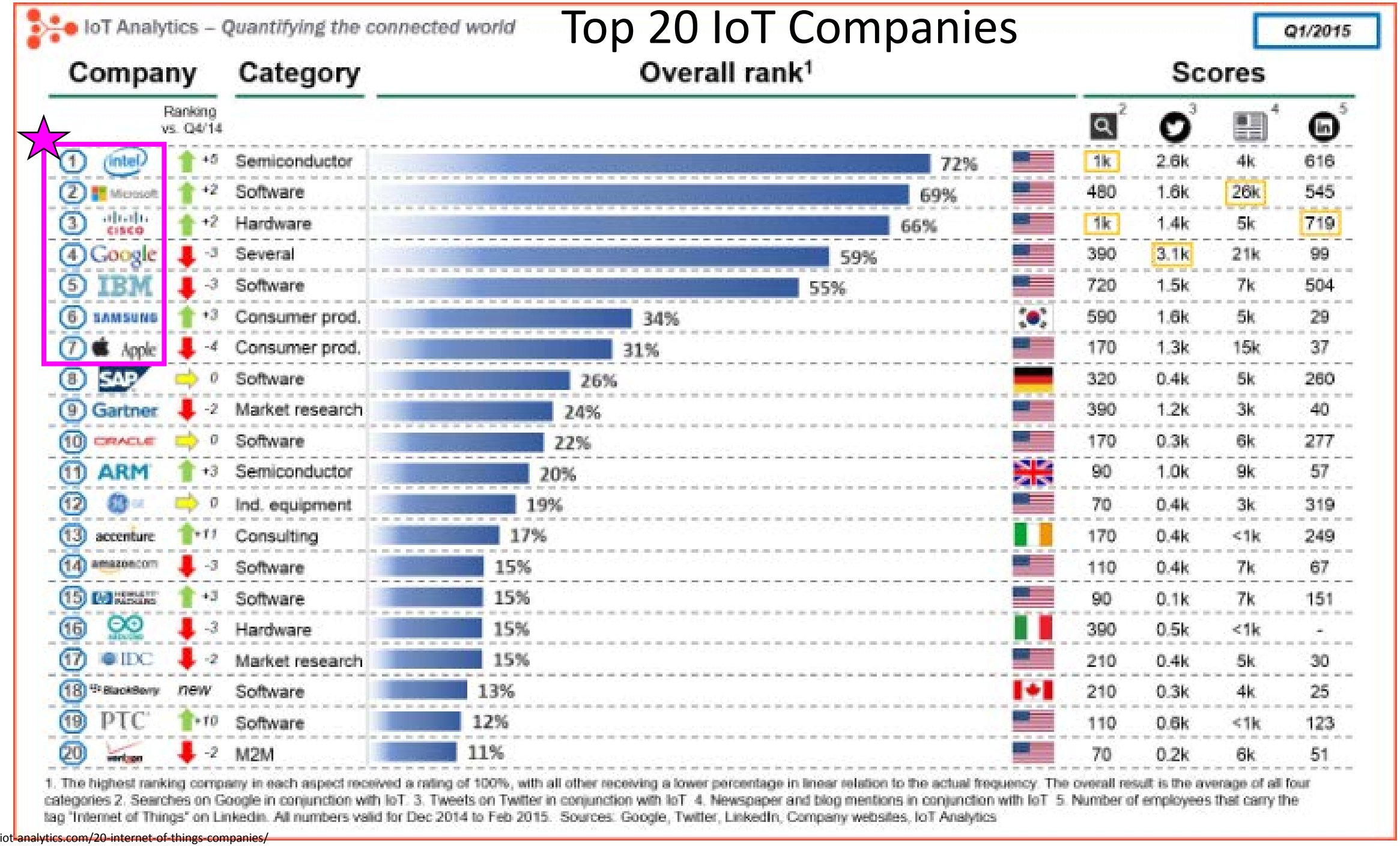
Apps, operating systems, & control hubs	Alibaba Amazon Apple Baidu Cisco Facebook GE Google IBM Microsoft Samsung Electronics Sony

http://www.slideshare.net/cmewawalla/the-internet-of-things-industry-trends-and-key-players



http://cen.vc/market/

Top 20 IoT Companies

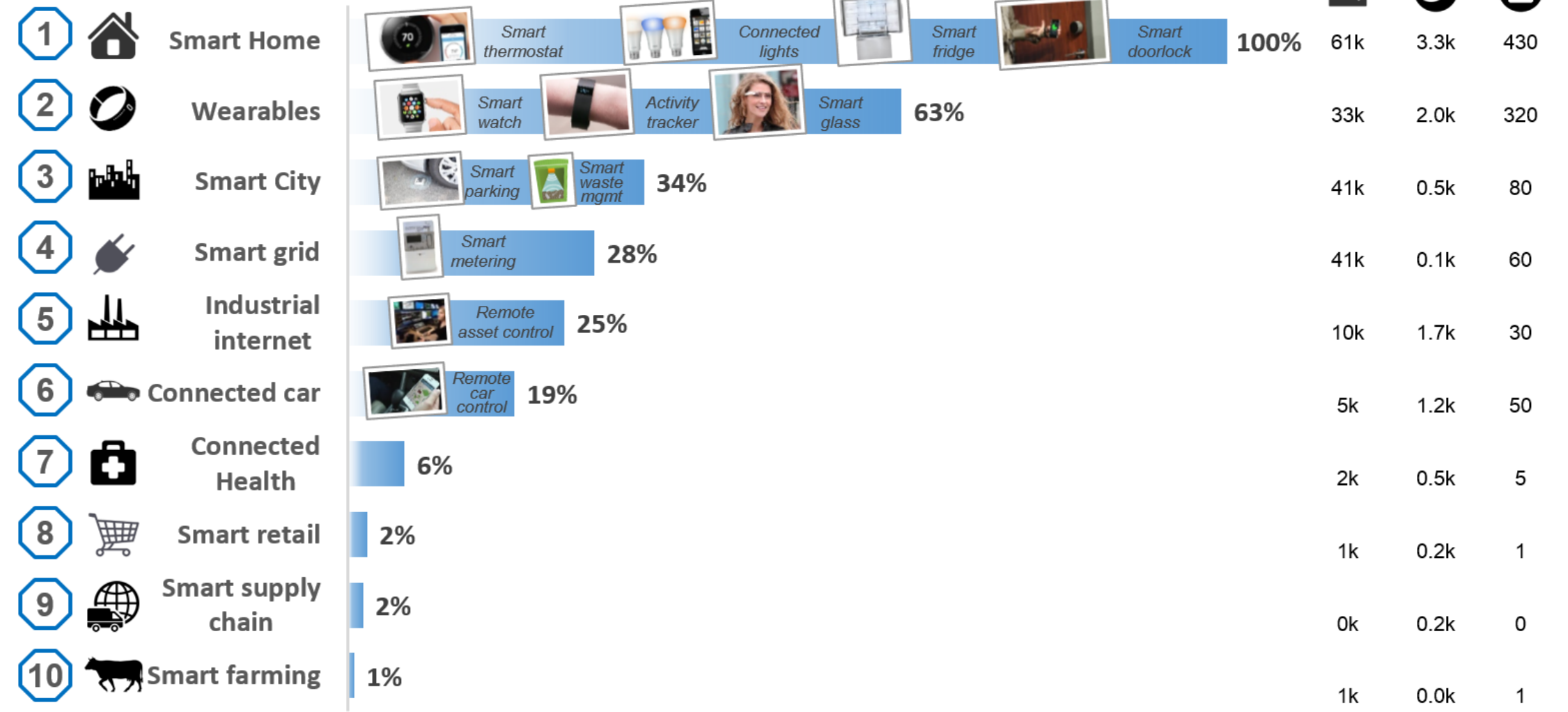


1. The highest ranking company in each aspect received a rating of 100%, with all other receiving a lower percentage in linear relation to the actual frequency. The overall result is the average of all four categories 2. Searches on Google in conjunction with IoT. 3. Tweets on Twitter in conjunction with IoT 4. Newspaper and blog mentions in conjunction with IoT 5. Number of employees that carry the tag "Internet of Things" on LinkedIn. All numbers valid for Dec 2014 to Feb 2015. Sources: Google, Twitter, LinkedIn, Company websites, IoT Analytics

http://iot-analytics.com/20-internet-of-things-companies/

Top 10 Most Popular IoT Applications

IoT Analytics – *Quantifying the connected world*



1. Monthly worldwide Google searches for the application 2. Monthly Tweets containing the application name and #IOT 3. Monthly LinkedIn Posts that include the application name. All metrics valid for Q4/2014.
Sources: Google, Twitter, LinkedIn, IoT Analytics

http://iot-analytics.com/10-internet-of-things-applications/

Overview

- Definition
- Standards
- Studies, Surveys
- Security and Privacy
  - World Economic Forum
  - White House Big Data Report
  - FTC
  - NIST Cyber-Physical Systems
  - Kaspersky
  - OWASP Internet of Things Top Ten Project & HP
  - Veracode
  - Wink
- Summary

World Economic Forum Warns About "Global Threat" of IoT Hacking

"We're inventing things faster than we can secure them. If Consumer Electronic Show told us anything, it's that every company is clamoring to plant a flag in this new emerging space. But this boom of what the WEF calls "hyperconectivity" along with the increase of cyber attack complexity, pushes cyber crimes as a highly likely and impactful risk for us all going forward."

http://gizmodo.com/global-risk-report-iot-hacking-becomes-a-bigger-threat-1680274553

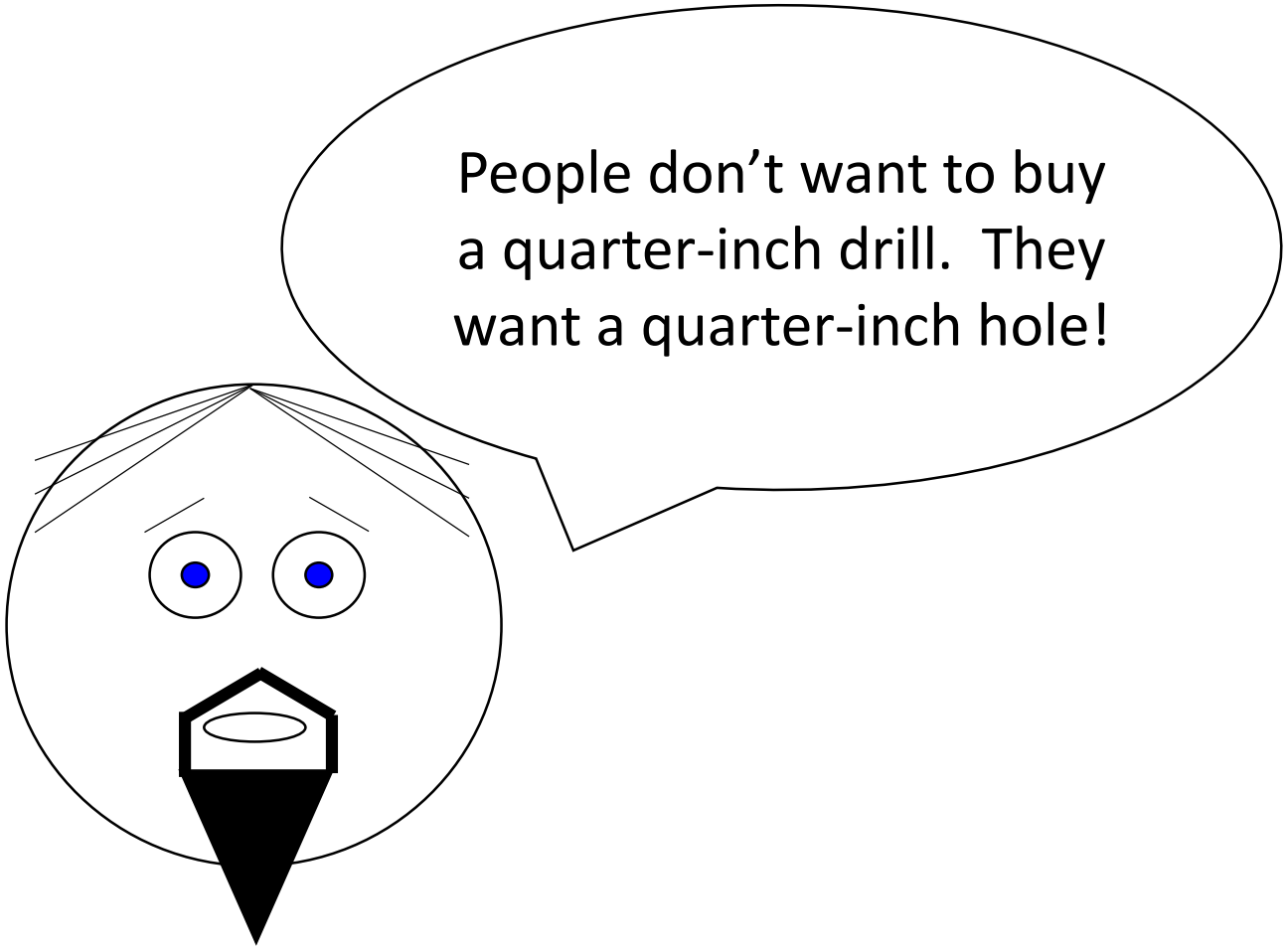
Figure 1: The Global Risks Landscape 2015

World Economic Forum

- *How will IoT impact existing industries, value chains, business models and work forces?*
- Value
  - New value from the massive volumes of data from connected products
  - Increased ability to make automated decisions and take actions in real time
- Business Opportunities
  - Operational efficiency – predictive maintenance and remote management (e.g. improved uptime, asset utilization)
  - Emergence of an outcome economy

http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

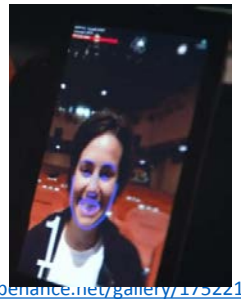
What is the “Outcome Economy”?



http://blog.iiconsortium.org/2015/03/industrial-internet-and-the-emergence-of-the-outcome-economy.html

What is an “Outcome Economy”?

- The ability of companies to create value by delivering solutions to customers that, in turn, lead to quantifiable results.
- “Hardware producing hard results”
- Examples
  - Pay Per Laugh - facial recognition technology is used to register each laugh and charges customers accordingly
  - Streetline smart parking sensors – connected parking spaces tell drivers where parking is available



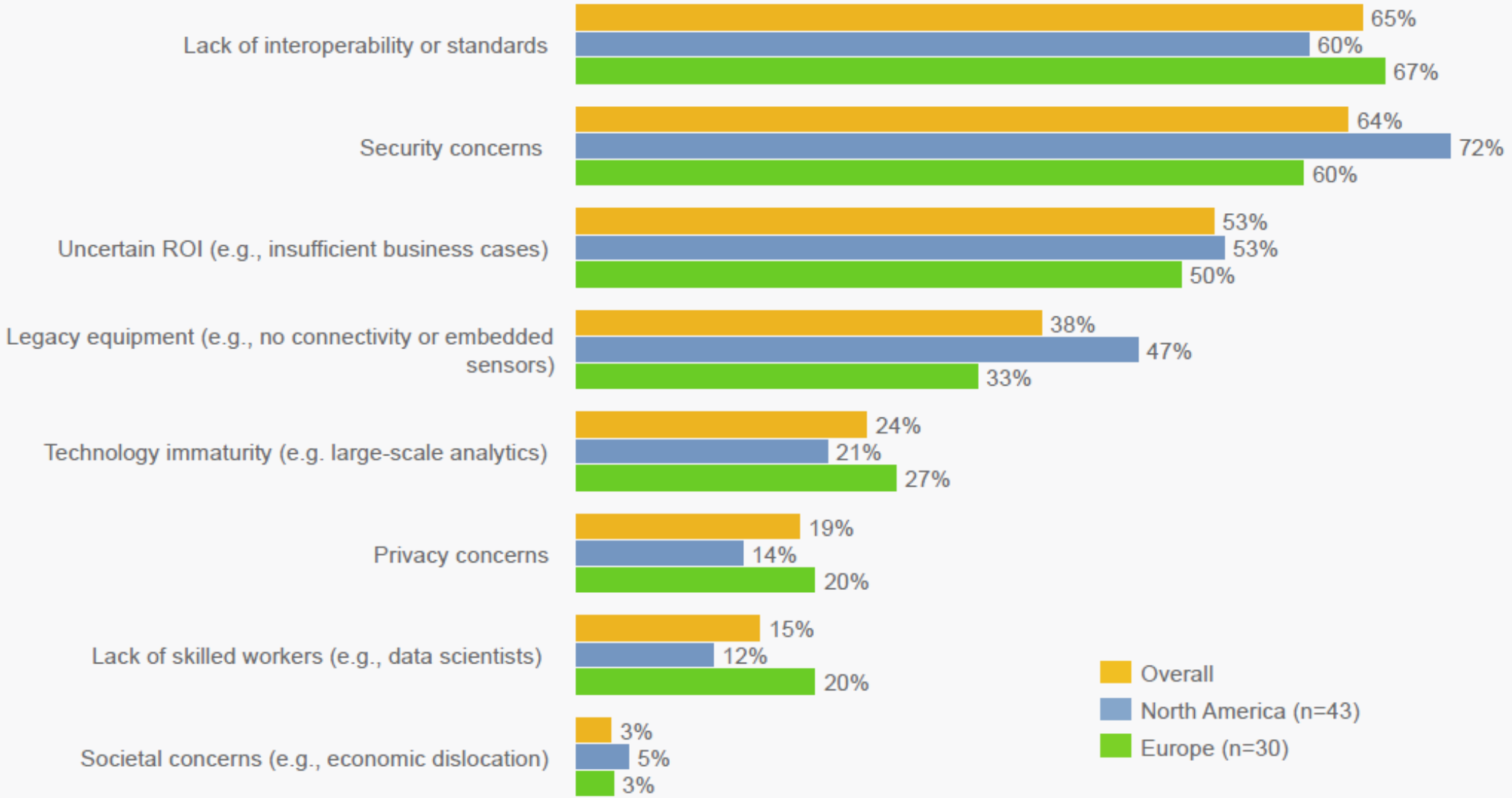
http://techtrends.accenture.com/us-en/bu v.behance.net/gallery/17522115/Pay-per-Laugh-TeatreNeumm http://www.streetline.com/blog/top-10-reasons-to-choose-streetline/

World Economic Forum - 2

- *How will IoT impact existing industries, value chains, business models and work forces?*
- Value
  - New value from the massive volumes of data from connected products
  - Increased ability to make automated decisions and take actions in real time
- Business Opportunities
  - Operational efficiency – predictive maintenance and remote management (e.g. improved uptime, asset utilization)
  - Emergence of an outcome economy - fueled by software-driven services, innovations in hardware and the increased visibility into products, processes, customers and partners
  - New connected ecosystem, coalescing around software platforms that blur traditional industry boundaries
  - Collaboration between humans and machines – resulting in unprecedented levels of productivity and more engaging work experiences
- Work forces
  - Growth in "digital labor" – smart sensors, intelligent assistants and robots
  - While lower-skilled jobs will be increasingly be replaced by machines, new, high-skilled jobs (e.g. medical robot designer, grid optimization engineer) will be created

http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

Q: What are the greatest barriers inhibiting business from adopting the industrial Internet?



Source: World Economic Forum Industrial Internet Survey, 2014

http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

White House Big Data Report

By senior Obama administration officials

- 3 Vs
  - Volume
    - Declining cost of collection, storage and processing of data, combined with new sources

> **What are the sources of big data?**
>
> The sources and formats of data continue to grow in variety and complexity. A partial list of sources includes the public web; social media; mobile applications; federal, state and local records and databases; commercial databases that aggregate individual data from a spectrum of commercial transactions and public records; geospatial data; surveys; and traditional offline documents scanned by optical character recognition into electronic form. The advent of the more Internet-enabled devices and sensors expands the capacity to collect data from physical entities, including sensors and radio-frequency identification (RFID) chips. Personal location data can come from GPS chips, cell-tower triangulation of mobile devices, mapping of wireless networks, and in-person payments.[12]

  - Variety
    - "Born digital" (e.g. computer, data processing system), "Born analog" (emanates from physical world), "data fusion" (brings together disparate sources of data)
  - Velocity
    - Increasingly approaching real time (e.g. users' online activities as interact with web pages, GPS data from mobile devices)

https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

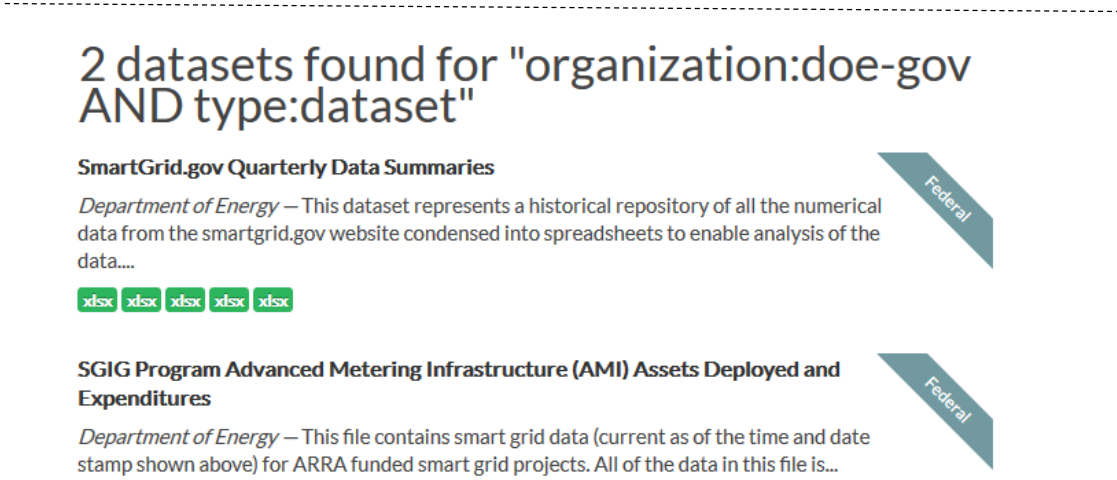
White House Big Data Report - 2

- Power and opportunity of Big Data
  - Internet of Things – merges the industrial and information economies
  - The Centers for Medicare and Medicaid Services – use predictive analytics software to flag likely instances of reimbursement fraud before claims are paid
  - Afghanistan war – DARPA deployed teams of data scientists and visualizers to the battlefield help commanders solve specific operational (e.g. fused satellite and surveillance data to visualize how traffic flowed through road networks making it easer to locate and destroy IEDs)
  - Synthesized data samples from monitors in a neonatal intensive care unit to determine which newborns were likely to contract potentially fatal infections

https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

7 Things to Know about the White House Big Data Report

- Big data is inevitable
- Big data is transformational at all levels of government
- Privacy needs reforms
- A new era of customized learning
- Predictive analytics is a start, but needs more
- Big data is the new national resource – e.g. requires secure storage
- Big data requires investment, resources



http://www.govtech.com/data/7-Things-to-Know-About-the-White-House-Big-Data-Report.html

Federal Trade Commission Staff Report Jan. 2015 – IoT Privacy & Security in a Connected World

- Mission
  - To prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity.
- Summarizes Nov. 2013 Workshop with 4 panels
  - "The Smart Home", "Connected Health and Fitness", "Connected Cars", "Privacy & Security in a Connected World"
- Benefits – numerous and potentially revolutionary benefits to consumers
  - Healthcare - Insulin pumps and blood-pressure cuffs connect to a mobile app can enable people to record, track and monitor their own vital signs without having to got to a doctor's office
  - Home – smart meters, "water bugs" (e.g. basements are flooded), oven and wine temperature monitoring
  - Connected cars – notify drivers of dangerous road conditions

https://www.ftc.gov/about-ftc, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Federal Trade Commission Staff Report Jan. 2015 – IoT Privacy & Security in a Connected World -2

- Risks
  - Security
    - Enable unauthorized access and misuse of personal information – e.g. smart TV
    - Facilitating attacks on other systems – e.g. launch DoS, send malicious emails
    - Creating safety risks – e.g. hack insulin pump and change settings, hack car's telematics' unit and control the vehicle's engine and braking, unauthorized access to fitness device data to track consumer's location and endanger physical safety
    - IoT market's lack of experience dealing with security issues
    - Devices which are inexpensive and essentially disposable may be difficult or impossible to update/apply software patch
  - Privacy
    - Volume of data is stunning (e.g. one home can generate 150 M discrete data points/day or one data point every 6 sec/household)
    - Smartphone sensors can be used to infer a user's mood, stress levels, personality type, bipolar disorder, demographics (e.g. gender, marital status, job status, age), smoking habits, overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercise, types of physical activity or movement
    - Companies can use this data to make credit, insurance and employment decisions

https://www.ftc.gov/about-ftc, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

FTC Recommendations

- Build security into devices from the beginning
- Train employees about the importance of security
- Ensure outside service providers are capable of maintaining reasonable security
- Use "defense-in-depth" security
  - Consider measure to prevent unauthorized access of consumer's device, data or personal information stored on the network
  - Monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks

https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices,http://privacylaw.proskauer.com/2015/02/articles/data-privacy-laws/ftc-issues-report-and-privacy-best-practices-for-the-internet-of-things/

Of Interest

- CPS Public Working Group (PWG)
- Big Data PWG
- Smart Grid
- Global City Teams Challenge - SmartAmerica Round Two
- Smart Manufacturing

CPS PWG Subgroups

- Reference Architecture
- Use Cases
- Timing
- Cybersecurity
- Data Interoperability

Related Links

- CPS Virtual Organization
- NSF CPS Program
- NSF CPS Projects
- FTC Internet of Things Workshop
- Industrial Internet Consortia (IIC)
- European Commission CPS

NIST Cyber-Physical Systems Workshop April 7-8, 2015 1 2 3 4

Welcome

Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, and electric power generation and delivery, as well as in many other areas now just being envisioned. Other phrases that you might hear when discussing these and related CPS technologies include:

- Internet of Things (IoT)
- Industrial Internet
- Smart Cities
- Smart Grid
- "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances)

The NIST Engineering Laboratory, through its Cyber-Physical Systems and Smart Grid Program Office, is leading a NIST-wide program to advance Cyber-Physical Systems. Our program is moving forward on three fronts:

Popular Links

- Cyber-Physical Systems Workshop
- Smart America
- Smart Grid Testbeds Measurement Challenges Workshop
- Smart Grid Homepage

Recent Developments

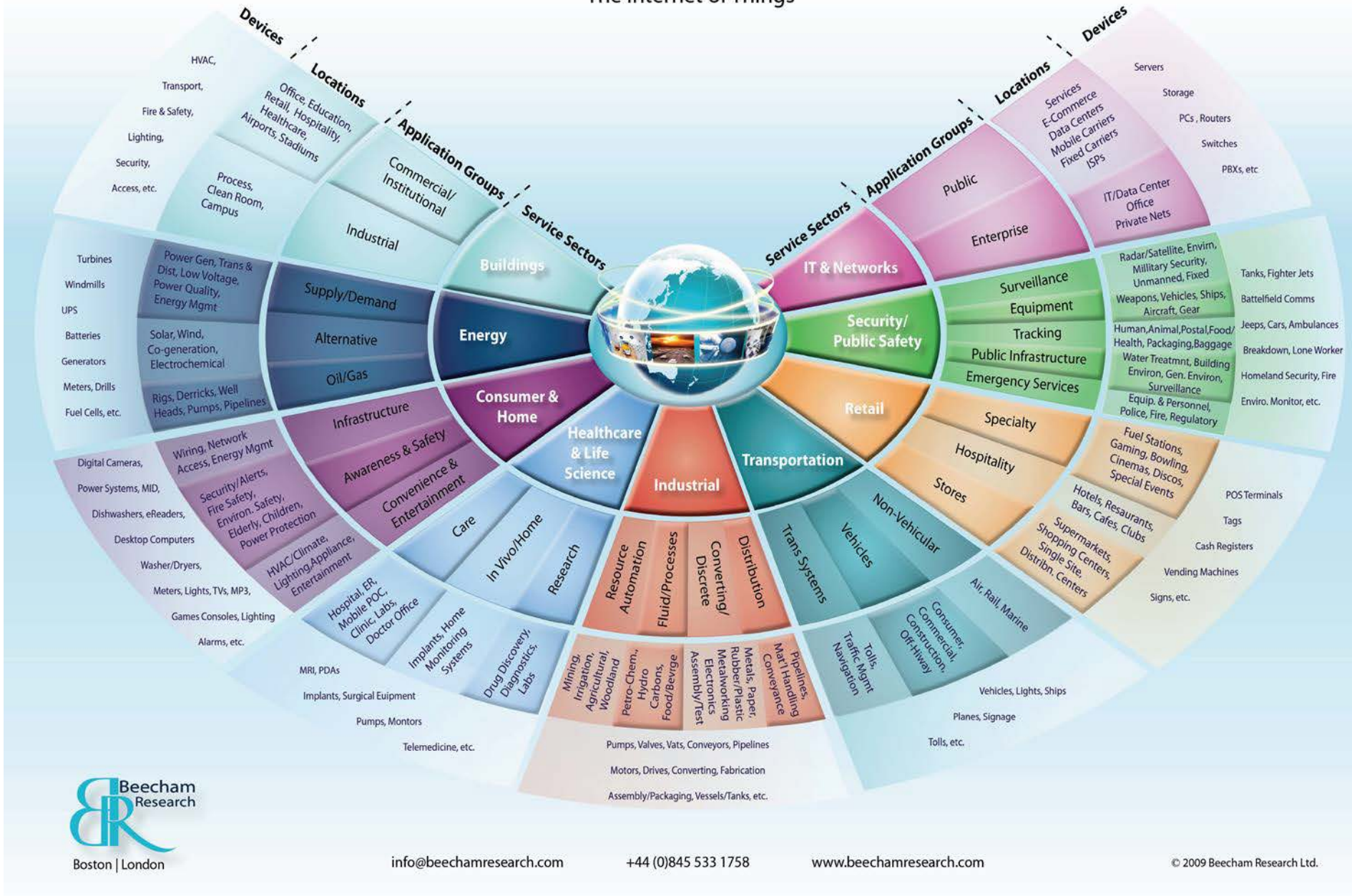
- Global City Teams Challenge Tech Jam (February 2015)
- Global City Teams Challenge Kick-off (September 2014)
- 08/11-12/2014 NIST Cyber-Physical Systems Public Working Group Workshop
- 06/30/2014 NIST Cyber-Physical Systems Public Working Group Kickoff Webinar
- 06/11/2014 The Internet's Next Big Idea: Connecting People, Information, and Things
- 06/11/2014 SmartAmerica Expo
- 06/10/2014 SmartAmerica Challenge: Harnessing the Power of the Internet of Things
- 04/04/2013 Designed-in Cybersecurity for Cyber-Physical Systems Workshop

The NIST Engineering Laboratory, through its Cyber-Physical Systems and Smart Grid Program Office, is leading a NIST-wide program to advance Cyber-Physical Systems. Our program is moving forward on three fronts:

- The Cyber-Physical Systems Public Working Group (CPS PWG), formed by NIST in 2014, brings together experts to help define and shape key aspects of CPS to accelerate its development and implementation within multiple sectors of our economy. Through its five subgroups, the CPS PWG is preparing a CPS Framework.

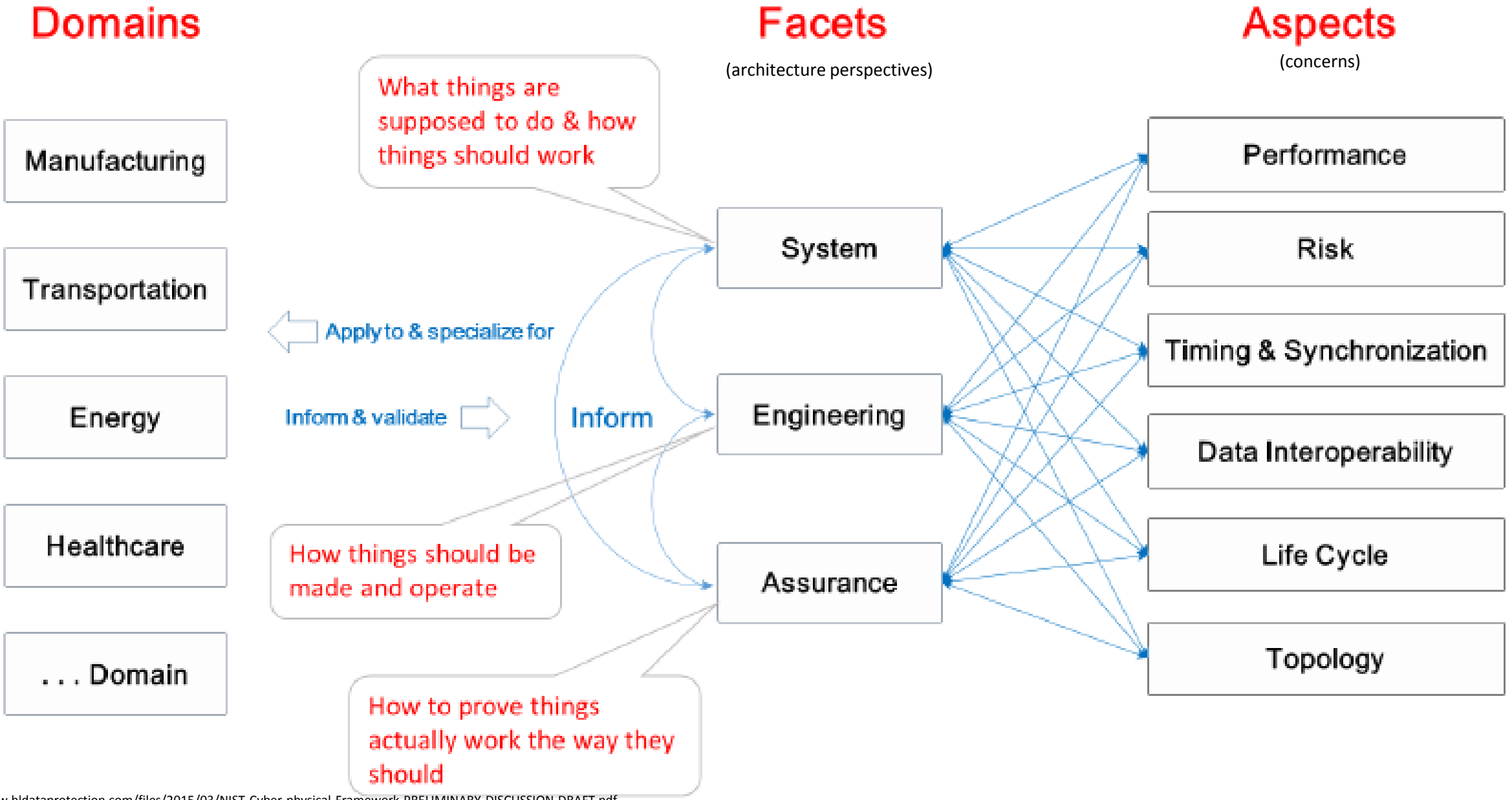
- The Global City Teams Challenge is a nine-month initiative to advance the deployment of Internet of Things (IoT) technologies within a smart city environment. More than 40 teams or "action clusters" are pursuing projects related to energy, transportation, public safety, and other key sectors.

- CPS research and standards development are carried out in multiple NIST Laboratories, including programs in advanced manufacturing, cybersecurity, buildings and structures, disaster resilience, and smart grid. A key goal for 2015 is to design and begin development of a CPS testbed to characterize CPS equipment, systems, performance, and standards.



http://www.hldataprotection.com/files/2015/03/NIST-Cyber-physical-Framework-PRELIMINARY-DISCUSSION-DRAFT.pdf

CPS Framework Reference Architecture



http://www.hldataprotection.com/files/2015/03/NIST-Cyber-physical-Framework-PRELIMINARY-DISCUSSION-DRAFT.pdf

Thu 5/7/2015 9:01 AM

Wollman, David A. <david.wollman@nist.gov>

RE: Cyber Physical System vs Internet of Things

To Frost, Sandy; nistcps

Hi Sandy,

The terms CPS and IoT are often used interchangeably to describe components, devices, and systems with similar characteristics - networked, connected objects that can sense, store, interpret, process or act on information or control devices in the physical world. We tend to see use of CPS by academic and government stakeholders, while private sector tends to use "industrial internet" or "IoT" for example in their marketing activities.

With respect to your additional questions, the objective of our CPS Public Working Group (CPS PWG) is to develop a shared understanding of CPS and its foundational concepts and unique dimensions to promote progress through exchanging ideas and integrating research across sectors and among disciplines and to support development of CPS with new functionalities. The CPS PWG is currently working on a Draft CPS Framework that captures the range of unique dimensions of CPS. The Draft CPS Framework not only addresses the unique dimensions of cybersecurity and privacy, but also an architectural methodology, use cases, and the importance of timing and data interoperability. SP 800-82 is focused on cybersecurity for industrial control systems, which can be seen as a subset of CPS. One of the differences between ICS and CPS relates to the concepts of composability and modularity. ICS, historically, have been purpose-built – that is, designed to fulfill a specific role. The envisioned future of CPS includes devices and components that can be used interchangeably for purposes that are yet to be defined.

Hope this helps .. and thanks for the questions, happy to receive input with your ideas as well.

Cheers,
Dave

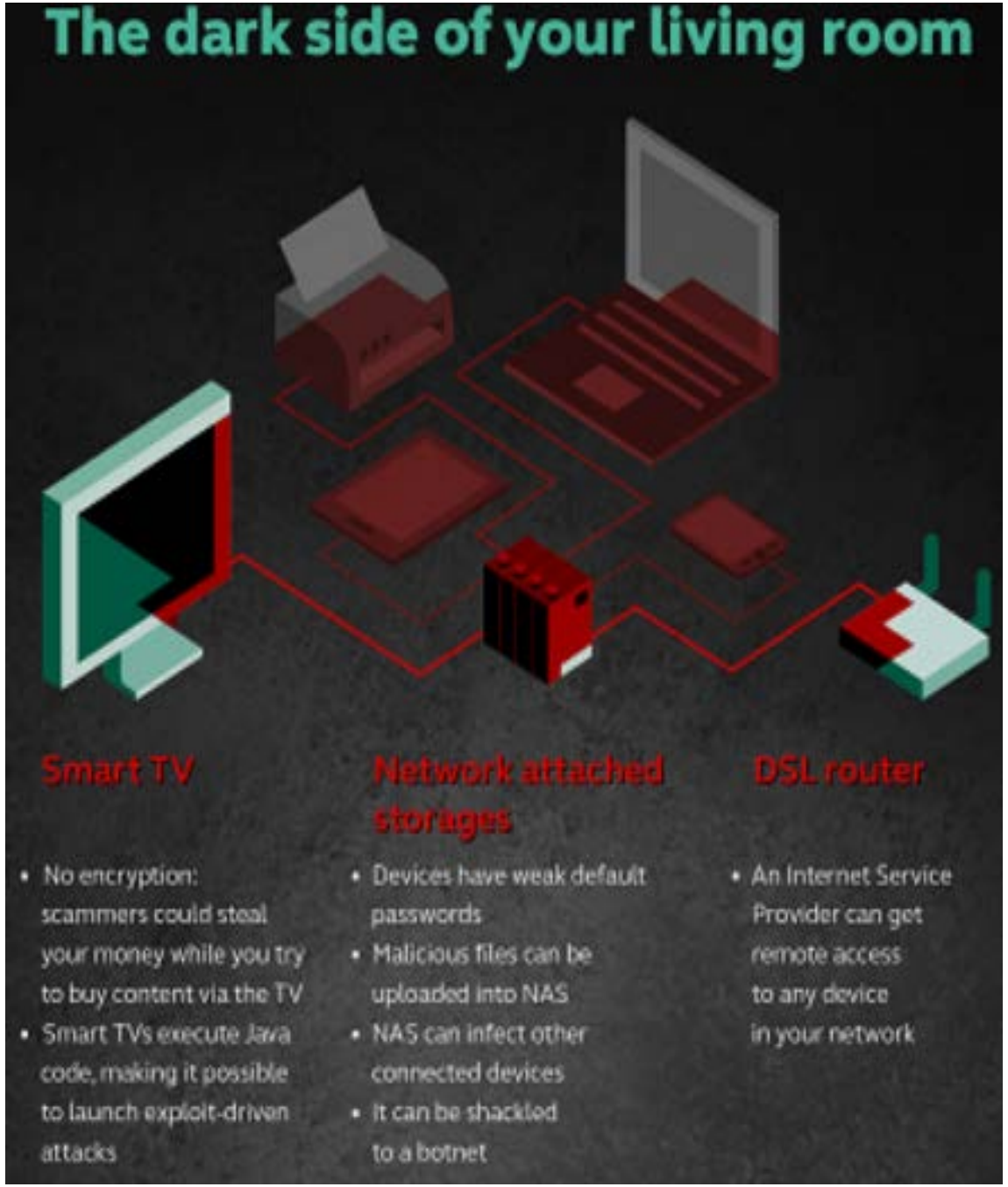
Dr. David Wollman
Deputy Director, Smart Grid and Cyber-Physical Systems Program Office
NIST
david.wollman@nist.gov

KASPERSKY lab

Internet of Crappy Things

February 19, 2015 Alex Drozhzhin Featured P

- David Jacoby - Attacked his home network
  - Equipment – NASs, smart TV, Satellite receiver, Router from ISP, printer
  - Got remote code execution on NAS in 20 min. using new vulnerability, found 22 vulnerabilities
  - Most IoT have web interface and use port 80 without https and use 192.168.0… addresses
  - Vendors not want to update devices – just buy a new one



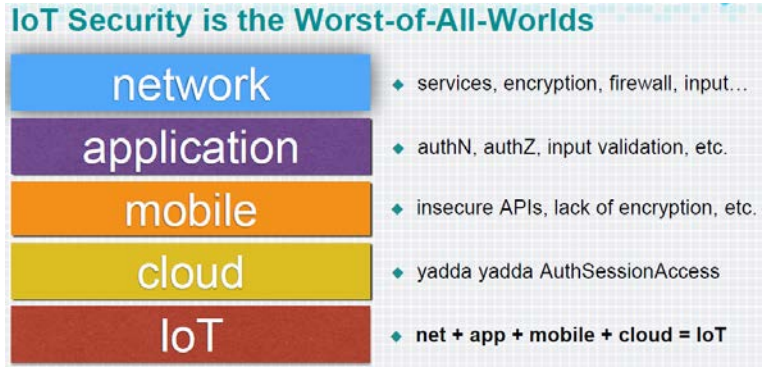
https://blog.kaspersky.com/internet-of-crappy-things/,https://t.co/ckTyeMVLUp,http://www.kaspersky.com/about/news/virus/2014/hacking-a-living-room,https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/

- Make sure all your devices are up to date with all the latest security and firmware updates. This is a problem for a lot of home business and entertainment devices, but it is still the best thing you can do to avoiding being at the mercy of known vulnerabilities. It also gives you an indication of whether the devices have any updates at all to install, or if it's considered to be a 'dead' product.
- Make sure that the default username and password are changed; this is the first thing an attacker will try when attempting to compromise your device. Remember that even if it's a 'stupid' product such as a satellite receiver or a network hard drive, the administrative interfaces are often vulnerable to serious vulnerabilities.
- Use encryption, even on the files you store in your network storage device. If you do not have access to an encryption tool, you can simply put your files in a password-protected ZIP file; it's still better than not doing anything at all.
- Most home routers and switches have the possibility to set up several different DMZ/VLAN. This means that you can setup your own 'private' network for your network devices, which will restrict network access to and from this device.
- Use common sense and understand that everything can be hacked, even your hardware devices.
- If you're really paranoid you can always monitor the outbound network traffic from these devices to see if there's anything strange going on, but this does require some technical knowledge. Another good tip is to restrict network devices from accessing sites they're not supposed to access, and only allow them to pull updates and nothing else.

https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/, https://www.youtube.com/watch?v=yhQMkQkMmSE

OWASP IoT Top Ten Project

- Daniel Miessler/HP Pen Tester
  - Too much focus on one device vulnerability instead of product (cloud, mobile app, network interface, SW, encryption, authentication, physical security, USB ports)



  - Then picked top 10 devices and used the Top 10 as foundation for their methodology (both consumer & corporate)

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf, http://www.databreachtoday.asia/interviews/10-risks-internet-things-security-i-2429, https://www.rsaconference.com/writable/presentations/file_upload/asd-t10-securing-the-internet-of-things-mapping-iot-attack-surface-areas-with-the-owasp-iot-top-10-project.pdf

The OWASP Internet of Things Top 10 - 2014 is as follows:

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

I9 | Insecure Software/Firmware

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device and/or the network the device resides on. Also consider anyone who could gain access to the update server.	Attacker uses multiple vectors such as capturing update files via unencrypted connections, the update file itself is not encrypted or they are able to perform their own malicious update via DNS hijacking. Depending on method of update and device configuration, attack could come from the local network or the internet.	The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. Security issues with software/firmware are relatively easy to discover by simply inspecting the network traffic during the update to check for encryption or using a hex editor to inspect the update file itself for interesting information.		Insecure software/firmware could lead to compromise of user data, control over the device and attacks against other devices.	Consider the business impact if data can be stolen or modified and devices taken control of for the purpose of attacking other devices. Could your customers be harmed? Could other users be harmed?

https://drive.google.com/file/d/0B52IUvO0LP6OZEpHalF3cDFlWWs/view

I9 | Insecure Software/Firmware | Testing

Is My Software/Firmware Secure?

- Note - It is very important that devices first and foremost have the ability to update and perform updates regularly.

Checking for insecure software/firmware updates include:

- Reviewing the update file itself for exposure of sensitive information in human readable format by someone using a hex edit tool
- Reviewing the production file update for proper encryption using accepted algorithms
- Reviewing the production file update to ensure it is properly signed
- Reviewing the communication method used to transmit the update
- Reviewing the cloud update server to ensure transport encryption methods are up to date and properly configured and that the server itself is not vulnerable
- Reviewing the device for proper validation of signed update files

Example Attack Scenarios

Scenario #1: Update file is transmitted via HTTP.

```
http://www.xyz.com/update.bin
```

Scenario #2: Update file is unencrypted and human readable data can be viewed.

```
ÐvÐñ]ÐÐúÐÐqwÐû]ÐÐ¯3DPÐóÐø]ÐÐ¯3DPadmin.htmadvanced.htmalarms.htm
```

In the cases above, the attacker is able to either capture the update file or capture the file and view it's contents.

- Encryption Not Used to Fetch Updates
- Update File not Encrypted
- Update Not Verified before Upload
- Firmware Contains Sensitive Information
- No Obvious Update Functionality

https://drive.google.com/file/d/0B52IUvO0LP6OZEpHalF3cDFlWWs/view

I9 | Insecure Software/Firmware | Make It Secure

How Do I Secure My Software/Firmware?

Securing software/firmware require:

1. Ensuring the device has the ability to update (very important)
2. Ensuring the update file is encrypted using accepted encryption methods
3. Ensuring the update file is transmitted via an encrypted connection
4. Ensuring the update file does not contain sensitive data
5. Ensuring the update is signed and verified before allowing the update to be uploaded and applied
6. Ensuring the update server is secure

Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer

https://drive.google.com/file/d/0B52IUvO0LP6OZEpHalF3cDFlWWs/view

Research findings

90 percent of devices collected at least one piece of personal information via the device, the cloud, or its mobile application.

Six out of 10 devices that provide user interfaces were vulnerabele to a range of issues such as persistent XSS and weak credentials.

80 percent of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.

IoT

XX%

70 percent of devices used unencrypted netwrok service.

70 percent of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

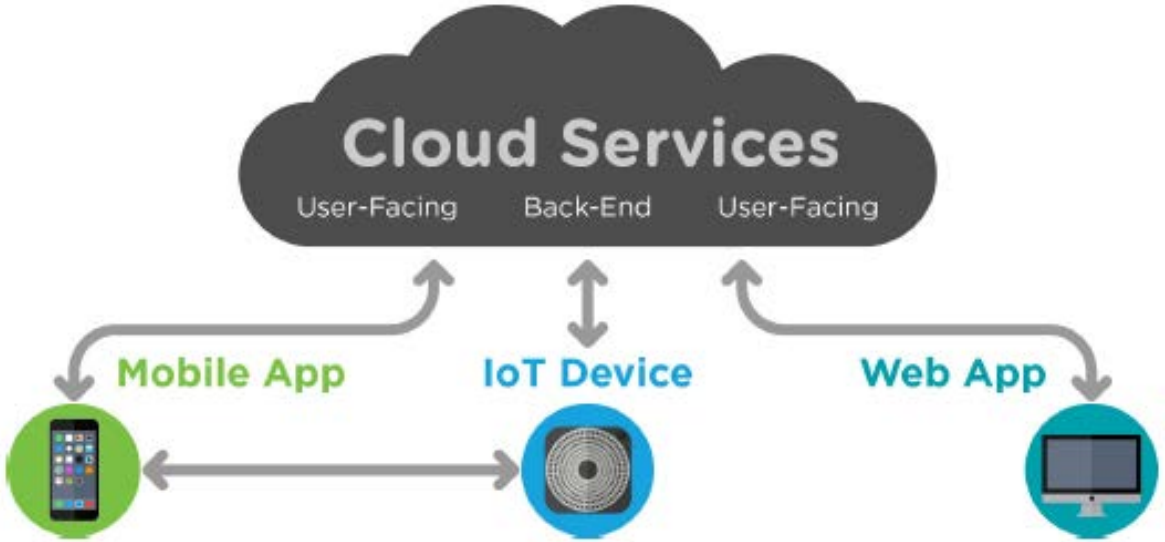
VERACODE
The Most Powerful Application Security Platform on the Planet

WHITE PAPER

Veracode Security Research Study

The Internet of Things: Security Research Study

- Examined 6 Internet-connected consumer devices across 4 different domains:



https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf?mkt_tok=3RkMMJWWfF9wsRogv63BZKXonjHpfsX87+8tWKW+lMI/0ER3fOvrPUfGjI4IScdlI+SLDwEYGJlv6SgFTbnFMbprzbgPUhA=

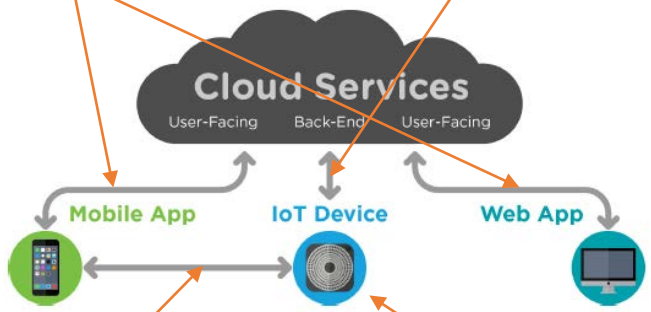
Authentication & Communication with User-Facing Cloud Services

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Cryptography Allowed	YES	YES	YES	YES	YES	YES
Cryptography Required	YES	YES	NO	YES	YES	YES
Strong Passwords	NO	NO	NO	YES	NO	NO
App SSL Validation	YES	YES	YES	YES	YES	YES

Enlarge Image

Authentication & Communication with Back-End Cloud Services

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Device-to-Service Authentication	YES	YES	YES	YES	YES	YES
Encryption Employed	YES	YES	NO	YES	NO	YES
Protection Against MITM	NO	NO (1)	NO (1)	YES	NO	NO
Sensitive Data Protected	YES	YES	NO	YES	N/A	YES
Replay Attack Protection	YES	YES	NO	YES	NO	NO



Mobile Application Interface

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Sensitive Data Secured	NO (1)	N/A	NO (1)	YES	NO (1)	N/A
TLS Validation	N/A	N/A	N/A	N/A	N/A	N/A

Device Debugging Interfaces

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Debugging Interfaces Restricted	NO (http)	NO (1) (ADB)	NO (ADB, VNC)	NO (telnet)	NO (http)	YES
Debugging Interfaces Secured	YES	NO	NO	YES	YES	YES
Arbitrary Code Restricted	YES	PARTIAL (2)	NO	YES	YES	YES

Enlarge Image

Voice Control Comes to the Forefront of the Smart Home

- Apple's iOs 8 HomeKit platform - Siri will control various 3rd party gadgets
- Amazon's Echo - see image
- ActiVocal's Vocca – lighting adapter
- Anthom's Homey – voice-activated version of Wink or SmartThings
- Honeywell's Thermostat
- Interactive Voice's Ivee Sleek – radio alarm clock+
- Ubi

http://www.cnet.com/news/voice-control-roundup/, http://www.amazon.com/oc/echo/, https://www.pinterest.com/source/theubi.com/

Results

- All but one device had vulnerabilities across most categories
  - Product manufactures not focused enough on security and privacy as a design priority
- Systems around which these devices were built depended heavily on their accompanying cloud services
  - For many, basic functionality can be disabled entirely by disrupting connectivity to the device's back-end cloud service
  - Virtually all commands from mobile applications are relayed through cloud services instead of being sent directly to devices

> Ubi's CEO Leor Grebler danced when I asked him for his response. "The report is an apples-to-oranges comparison. The Ubi is not a 'common at-home device' -- we were a Kickstarter-backed product and putting it next to Wink and MyQ is flattering." If the report was about marketing spend and units shipped, he might have a point, but the Ubi is for sale to consumers, and that's all that matters. Grebler does mention in **a forum post** that beefing up password protection is "on our roadmap," but the overall tone of his response is more defensive than reassuring.

http://www.cnet.com/news/security-study-highlights-vulnerabilities-in-popular-smart-home-devices/

Wink smart home hubs knocked out by security certificate

April 19, 2105

Now for the downside of a house loaded up with "smart" devices to allow remote control and monitoring: turning your home into a computer means computer-like problems. Today's example comes from the Wink Hub, a $50 device sold at Home Depot that's supposed to simplify things by working across standards and link common home appliances (lights, thermostat, garage door, etc.) to your phone. That was the plan until yesterday when Wink ~~sent out a software update~~ that went wrong somehow, and now a number of users have a box "so secure that it is unable to connect to the Wink servers" (Wink's words, not ours). The problem knocked all Wink hubs offline from 12:40PM to 11PM ET yesterday, and while the company says a "majority" of hubs were able to recover and reconnect, those that weren't will need to be sent back.

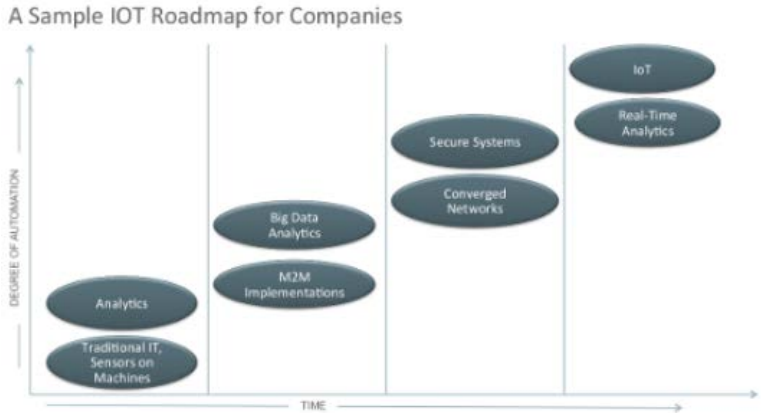
Update: We've confirmed what several Wink users have reported -- it appears that an expired certificate is at the root of the problem. The update pushed out was an attempt to fix the issue, and judging by responses on the Facebook group it did work for some owners. Stay tuned though, we're expecting more information on the issue shortly. [Thanks, Paul!]

http://www.engadget.com/2015/04/19/wink-home-automation-hub-bricked/,http://pureimage.ca/why-you-should-keep-your-home-automation-at-home-and-not-in-the-cloud/

Overview

- Definition
- Standards
- Studies, Surveys
- Security and Privacy
- Summary

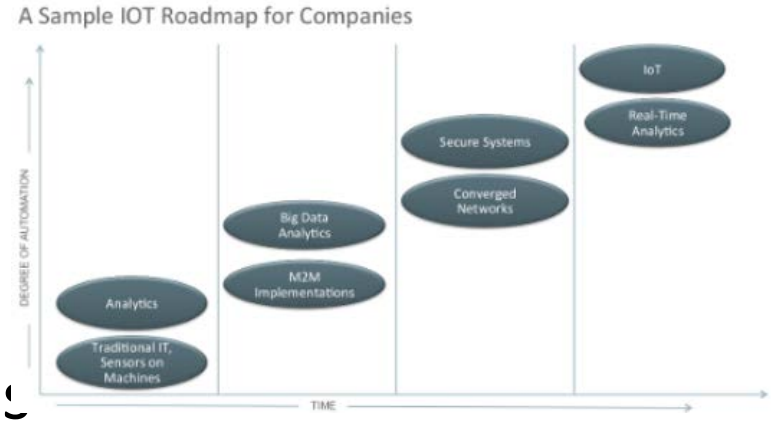
Summary



- Identify/appoint an individual to lead IoT initiatives
- Develop philosophies (e.g. holistic approach, business case benefits, applicable standards and regulations, life cycle analysis, data integration, time frame)
- Scope project
  - Identify sectors/applications that could benefit from IoT developments short and long term
  - Estimate implementation requirements (e.g. brown/greenfield, infrastructure, bandwidth, data, privacy, security, application development, support, training, policies, business processes, vendor capabilities)
  - Identify IT/OT requirements (e.g. infrastructure, security, bandwidth, applications, hosted solutions, analytical capabilities, equipment)
  - Create Roadmap
- Develop education plan

http://www.forbes.com/sites/gartnergroup/2015/02/26/corporate-leaders-arent-prepared-for-the-internet-of-things/,http://www.forbes.com/sites/oracle/2015/04/28/7-important-points-in-preparing-for-the-internet-of-things/,
http://www.zdnet.com/article/preparing-for-the-internet-of-things/,http://www.oracle.com/us/corporate/profit/big-ideas/081214-siyer-2264337.html

Summary



- Identify/appoint an individual to lead IoT initiatives
- Develop philosophies (e.g. holistic approach, business case benefits, applicable standards and regulations, life cycle analysis, data integration, time frame)
- Scope project
  - Identify sectors/applications that could benefit from IoT developments short and long term
  - Estimate implementation requirements (e.g. brown/greenfield, infrastructure, bandwidth, data, privacy, security, application development, support, training, policies, business processes, vendor capabilities)
  - Identify IT/OT requirements (e.g. infrastructure, security, bandwidth, applications, hosted solutions, analytical capabilities, equipment)
  - Create Roadmap
- Develop education plan