Key Aspects of Cybersecurity in the context of Internet of Things (IOT)

Raj Kumar

Key Aspects of Cybersecurity in the context of Internet of Things (IOT)

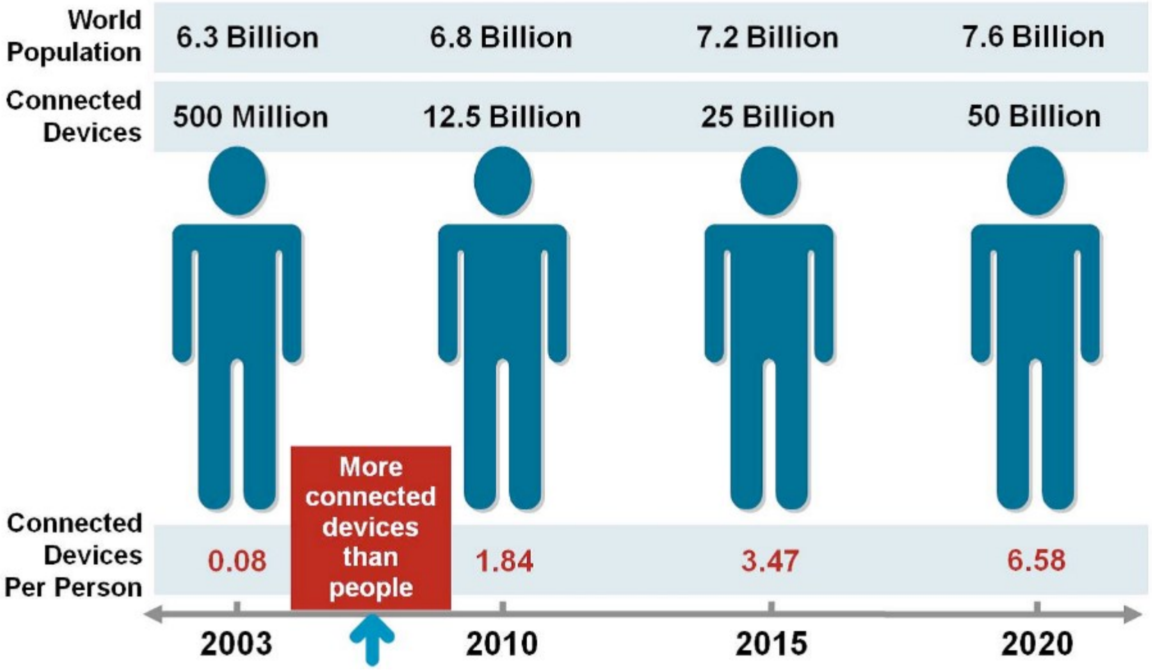
- IoT Security Challenges and Recent Incidents
- The legal liability in the IoT
- Industrial IoT Security

Key Aspects of Cybersecurity in the context of Internet of Things

"The Internet of Things(IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M)and covers a variety of protocols, domains, and applications. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue." Wikipedia

Connected devices

- 50 billion connected devices by 2020
- More than 6 connected devices per Person
- $1.7 trillion in value added to the global economy in 2019
- By 2020, IoT will be more than double the size of the smartphone, PC, tablet, connected car, and the wearable market combined.
- Technologies and services generated global revenues of $4.8 trillion in 2012 and will reach $8.9 trillion by 2020, growing at a compound annual rate (CAGR) of 7.9%.

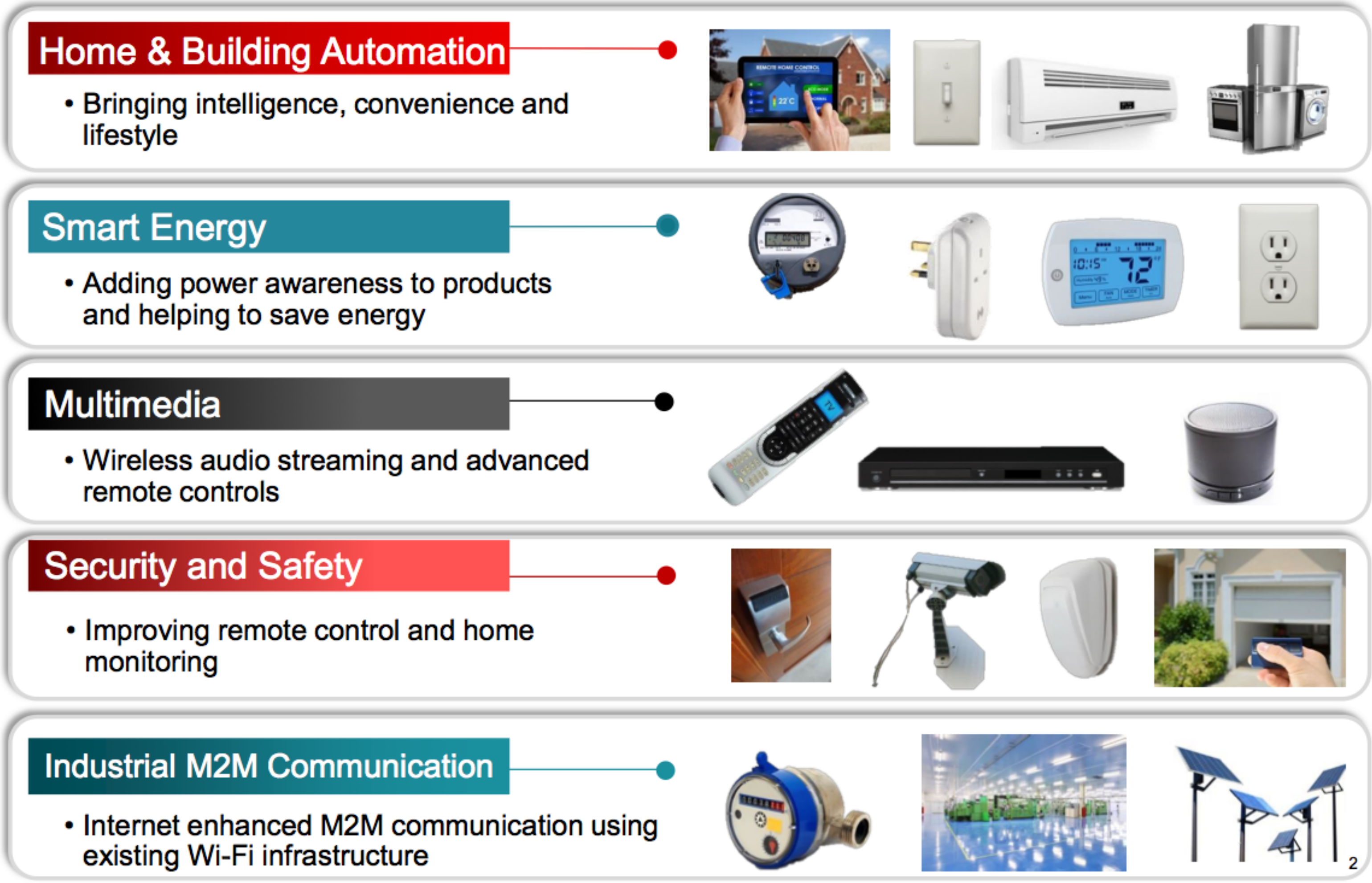


	2003	2010	2015	2020
World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58

More connected devices than people

Source: Cisco IBSG, April 2011

IoT devices and uses



Home & Building Automation

- Bringing intelligence, convenience and lifestyle

Smart Energy

- Adding power awareness to products and helping to save energy

Multimedia

- Wireless audio streaming and advanced remote controls

Security and Safety

- Improving remote control and home monitoring

Industrial M2M Communication

- Internet enhanced M2M communication using existing Wi-Fi infrastructure

http://eecatalog.com/caciufo/wp-content/uploads/2014/06/IoT-devices.png

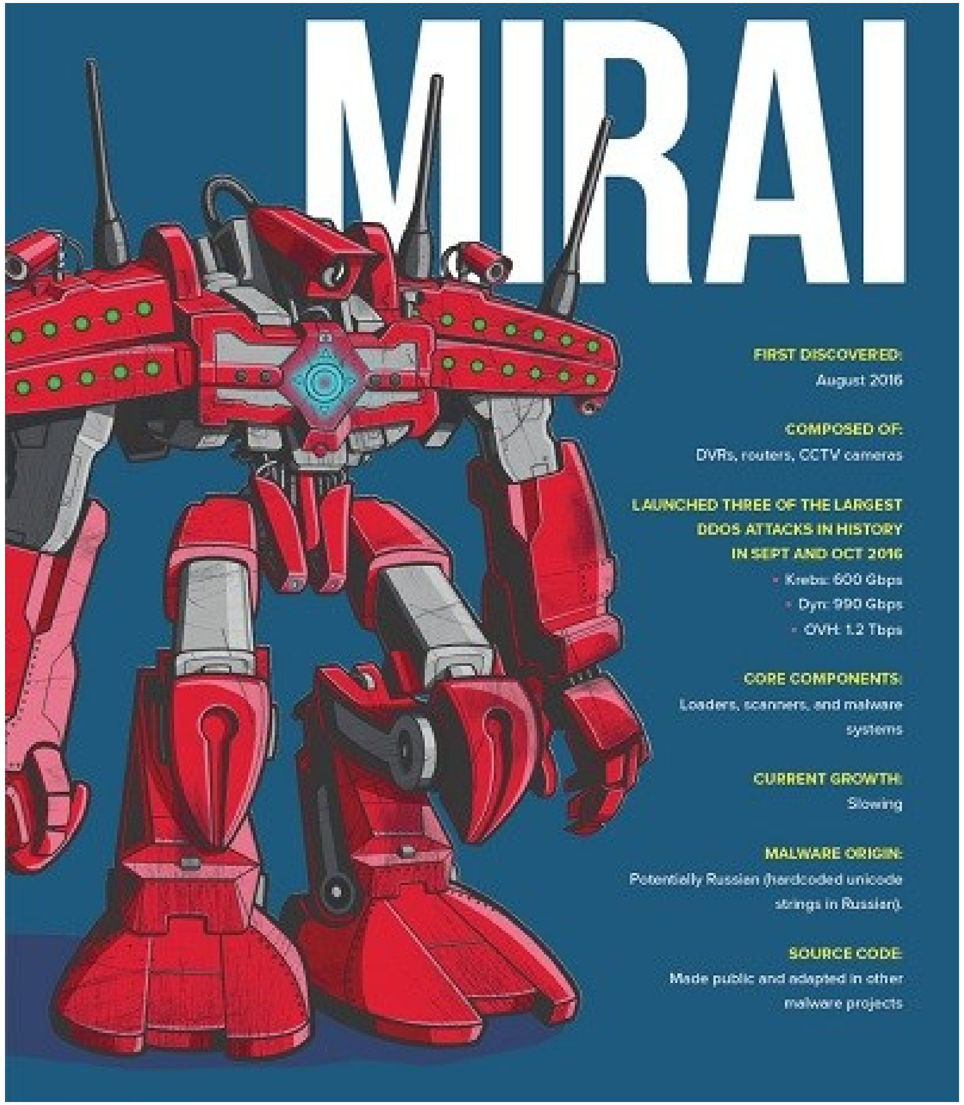
Industry sector that use IoT

1. Manufacturing
2. Transportation
3. Retail
4. Science and Technology
5. IT and Communications
6. Education
7. Healthcare
8. Energy
9. Construction
10. Agriculture

Recent Incidents

Botnet:

- A ThingBot is a botnet consisting of devices within the Internet of things.
- Vulnerable or infected appliances that are connected to the Internet can potentially pose a risk to corporate networks (Kaspersky).
- Number of attacks against Routers, SmartTV, network-attached storage devices, gaming consoles and various types of set-top boxes is increasing.
- Many set-top boxes runs on embedded linux or apache operating systems of ARM-like microcomputers.



FIRST DISCOVERED:
August 2016

COMPOSED OF:
DVRs, routers, CCTV cameras

LAUNCHED THREE OF THE LARGEST DDOS ATTACKS IN HISTORY IN SEPT AND OCT 2016
- Krebs: 600 Gbps
- Dyn: 990 Gbps
- OVH: 1.2 Tbps

CORE COMPONENTS:
Loaders, scanners, and malware systems

CURRENT GROWTH:
Slowing

MALWARE ORIGIN:
Potentially Russian (hardcoded unicode strings in Russian).

SOURCE CODE:
Made public and adapted in other malware projects

https://f5.com/Portals/1/Images/userfiles/290207/IoT_Vol3_Embed4_400px.jpg

Abuses of IoT devices

Computational capabilities, increasing capabilities of microcomputers and Internet connection makes IoT devices a privileged attack tool for hackers.

IoT devices could be used to:

- Send Spam.
- Coordinate an attack against a critical infrastructure.
- Serve a malware.
- Work as entry point within a corporate network.

Sample of Linux worm targeting IoT devices

- In November 2013 Symantec detected the worm Linux.Darllozexploitingthe PHP vulnerability CVE-2012-1823 to propagate itself.
- The Linux.Darlloz infected Home internet kits with x86 chips (i.e.routers) and were discovered variant for ARM, PPC, MIPS and MIPSEL architectures.
- The worm:
  - generates random IP addresses and attempts to use commonly used credentials to log into the target machine.
  - It sends HTTP POST requests specifically crafted, once compromised the target it downloads the worm from a C&C server and starts searching for other targets.
  - Once the worm has compromised a device, it kills off access to any Telnet services running.
  - Change default settings, adopt strong password, keep updated the software and firmware.

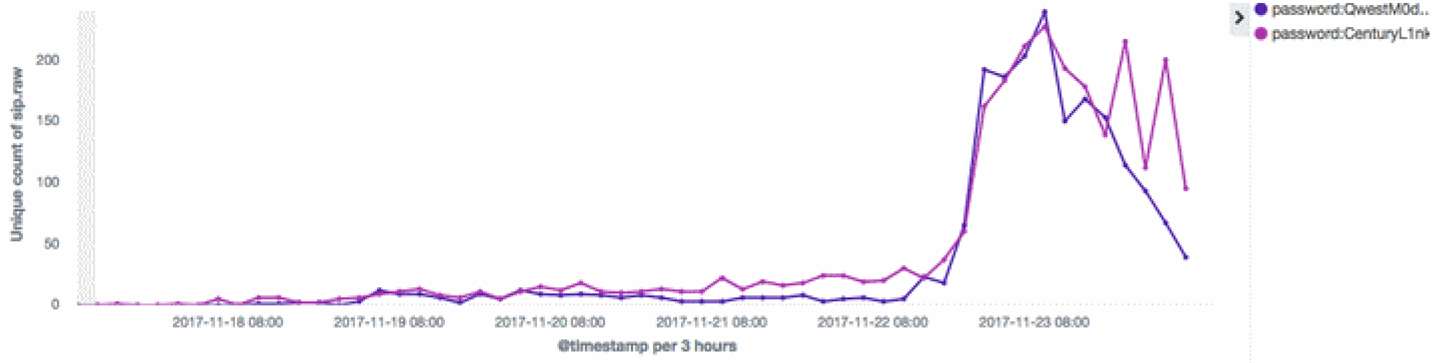
Large number of attack on IoT devices

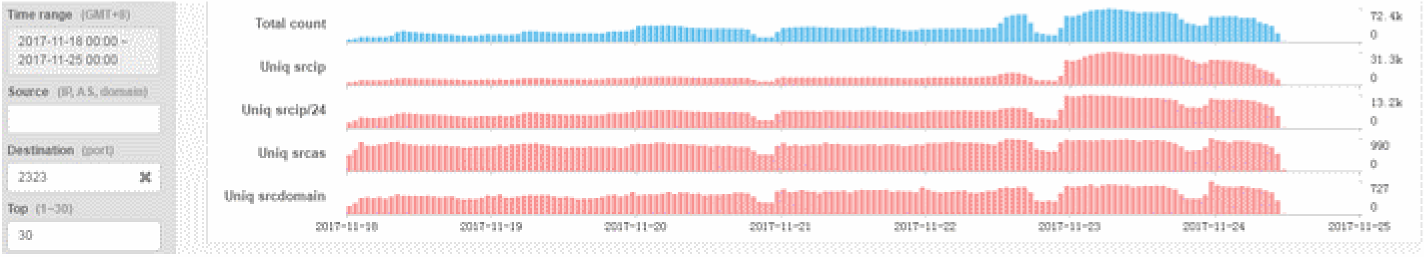
- Proofpoint discovered more than 750,000 Phishing and SPAM Emails launched From “Thingbots” used in an attack against a critical infrastructure from anywhere in the globe
- Cyber criminals sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide
- More than 100,000 Refrigerators, Smart TVs and other smart household appliances have been hacked.
- No more than 10 emails were initiated from any single IP address.

“Bot-nets are already a major security concern and the emergence of thingbots may make the situation much worse,” “Many of these devices are poorly protected at best and consumers have virtually no way to detect or fix infections when they do occur. Enterprises may find distributed attacks increasing as more and more of these devices come on-line and attackers find additional ways to exploit them.” said ***David Knight, General Manager of Proofpoint’s Information Security division.***

Mirai attack on IoT devices

A new Mirai variant is rapidly spreading, experts observed around 100K IPs running the scans in the past 60 hours searching for flawed ZyXEL PK5001Z routers - November 2017





Time range (GMT+8)
2017-11-18 00:00 ~
2017-11-25 00:00

Source (IP, A.S, domain)

Destination (port)
2323 ✖

Top (1~30)
30

http://securityaffairs.co/wordpress/66012/malware/mirai-argentina.html

Botnet runs DDoS from IoT devices

- Akamai spotted a Spike malware which is used to run DDoS attacks through desktops and IoT devices.
- Spike toolkit is able to generate an ARM-based payload
- The spike botnet was composed by routers, smart thermostats, smart dryers, freezers, Raspberry Pi and other IoT devices.
- Spike botnet composed by 12,000 -15,000 devices (sept 2014).
- One of the attack clocked 215 Gbps and 150 million packets per second (Mpps).
- SNORT signature analysis suggested to mitigate application-layer GET flood attacks.

IoT – OWASP Top Ten - 2014

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

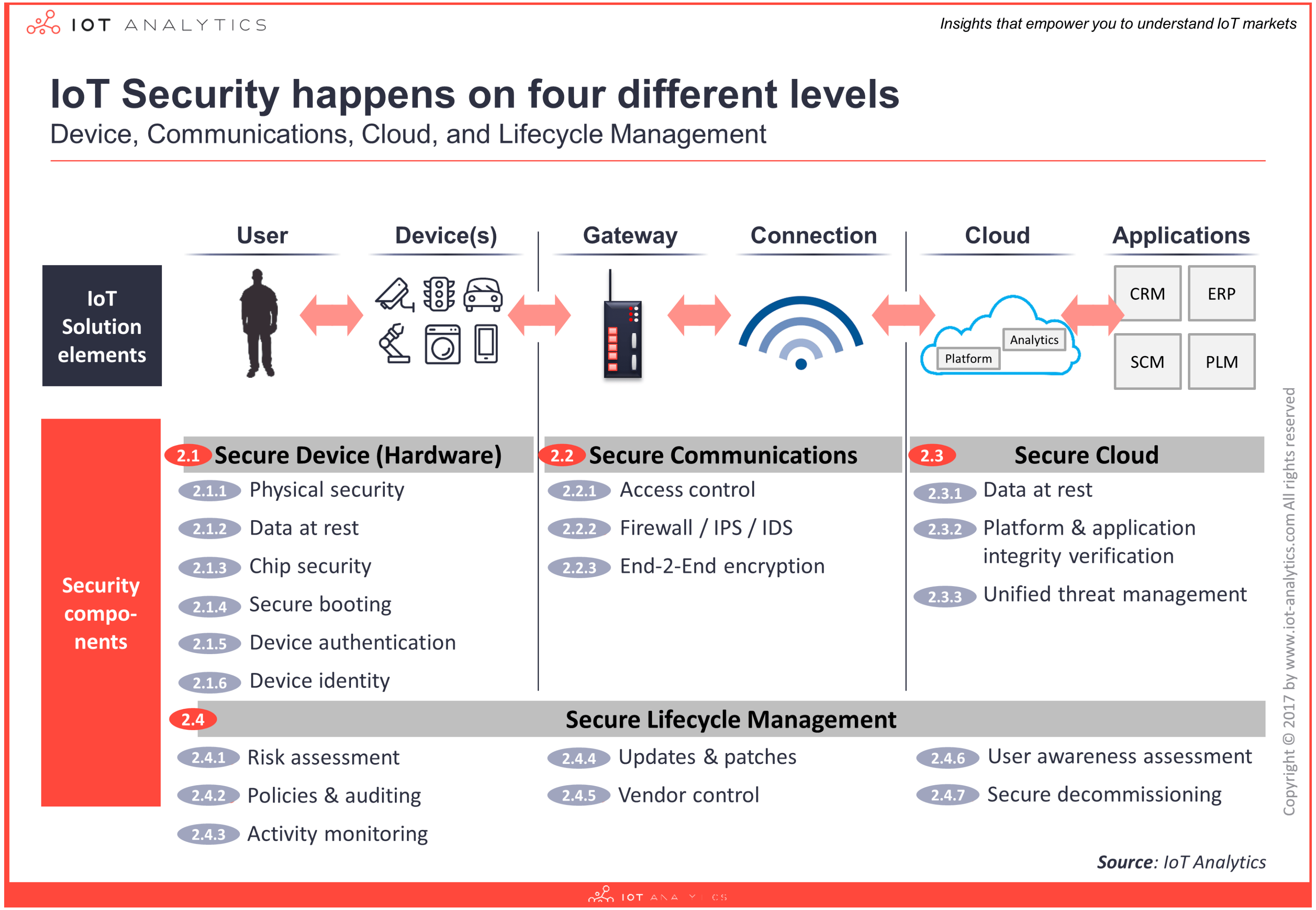
age
Discussion
Main
OWASP Internet of Things Top 10 for 2014
Project Details
OWASP
Open Web Application Security Project

OWASP Internet of Things Top Ten Project

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

IoT Security



IOT ANALYTICS

Insights that empower you to understand IoT markets

IoT Security happens on four different levels

Device, Communications, Cloud, and Lifecycle Management

Security compo- nents

2.1 Secure Device (Hardware)

- 2.1.1 Physical security
- 2.1.2 Data at rest
- 2.1.3 Chip security
- 2.1.4 Secure booting
- 2.1.5 Device authentication
- 2.1.6 Device identity

2.2 Secure Communications

- 2.2.1 Access control
- 2.2.2 Firewall / IPS / IDS
- 2.2.3 End-2-End encryption

2.3 Secure Cloud

- 2.3.1 Data at rest
- 2.3.2 Platform & application integrity verification
- 2.3.3 Unified threat management

2.4 Secure Lifecycle Management

- 2.4.1 Risk assessment
- 2.4.2 Policies & auditing
- 2.4.3 Activity monitoring
- 2.4.4 Updates & patches
- 2.4.5 Vendor control
- 2.4.6 User awareness assessment
- 2.4.7 Secure decommissioning

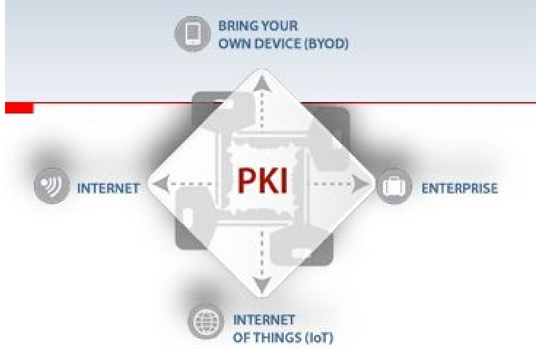
Source: *IoT Analytics*

IOT ANALYTICS

IoT Security Challenges

- Demand of connectivity for the Internet of Things(IoT) exploding.
- The global network must be able to securely and efficiently handle all these connections.
- Lack of standardization in the IoT market.
- Every single connection could make networks vulnerable.
- Every connected device has a network address. Internet Protocol (IPv6) extends the addressing space
- DNS will play an even more central role with the diffusion of M2M connections.
- Organizations will need to improve security and prevent DDoS and cache poisoning attacks.

IoT Security Challenges



PKI can help to improve IoT Security:

- IoT devices communicate among themselves with little human interaction, mutual authentication is a crucial aspect of the paradigm.
- Prevent leakage of personal information and harmful actuating tasks by means of peer authentication and secure data transmission.
- Recent attacks like the “smart” light bulb password leaks, hacks of Foscam baby monitors, Belkin home automation systems, and hacks of smart cars systems are just the beginning.
- PKI-based solutions could help to secure exchanging information across the Internet and mutual authenticate the actors.
- •PKI is already being used to address problems similar to the ones the Internet.

Industrial IoT Security

- The term Industrial Internet of Things (IIoT) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT.
- IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0.
- It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce.
- The potential of growth by implementing IIoT will generate $12 trillion of global GDP by 2030

Industrial Internet Consortium

- Launched in 2014 – now with over 258 members (Nov, 2016)
- The Industrial Internet Consortium is a global, member supported program that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.
- The Industrial Internet Consortium was founded by five companies: AT&T, Cisco, General Electric, Intel, and IBM.

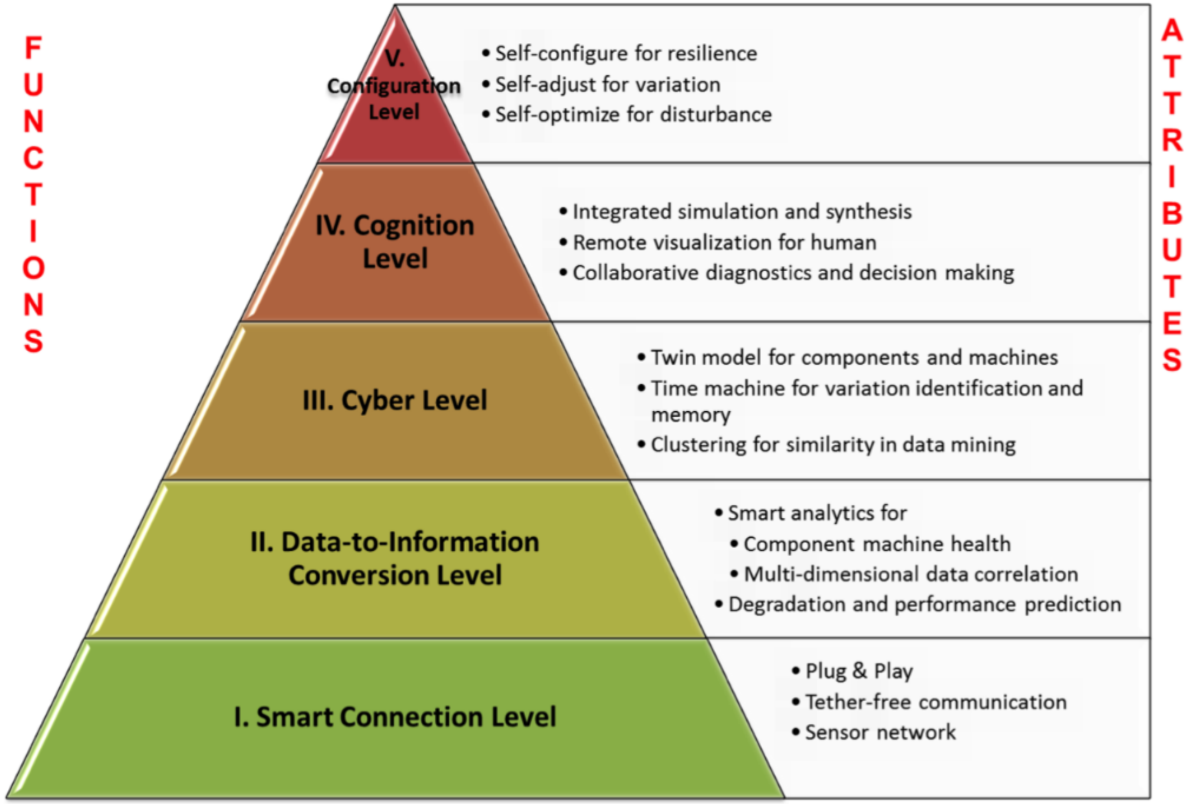
http://www.iiconsortium.org/

250+ Member Organizations
Spanning 28 Countries

Industrial IoT

- Network control and management of manufacturing equipment, asset and situation management, or manufacturing process brings IoT to industrial applications and smart manufacturing

- The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.



FUNCTIONS

ATTRIBUTES

V. Configuration Level
- Self-configure for resilience
- Self-adjust for variation
- Self-optimize for disturbance

IV. Cognition Level
- Integrated simulation and synthesis
- Remote visualization for human
- Collaborative diagnostics and decision making

III. Cyber Level
- Twin model for components and machines
- Time machine for variation identification and memory
- Clustering for similarity in data mining

II. Data-to-Information Conversion Level
- Smart analytics for
  - Component machine health
  - Multi-dimensional data correlation
- Degradation and performance prediction

I. Smart Connection Level
- Plug & Play
- Tether-free communication
- Sensor network

Industrial IoT

- Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT.

- Asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability.

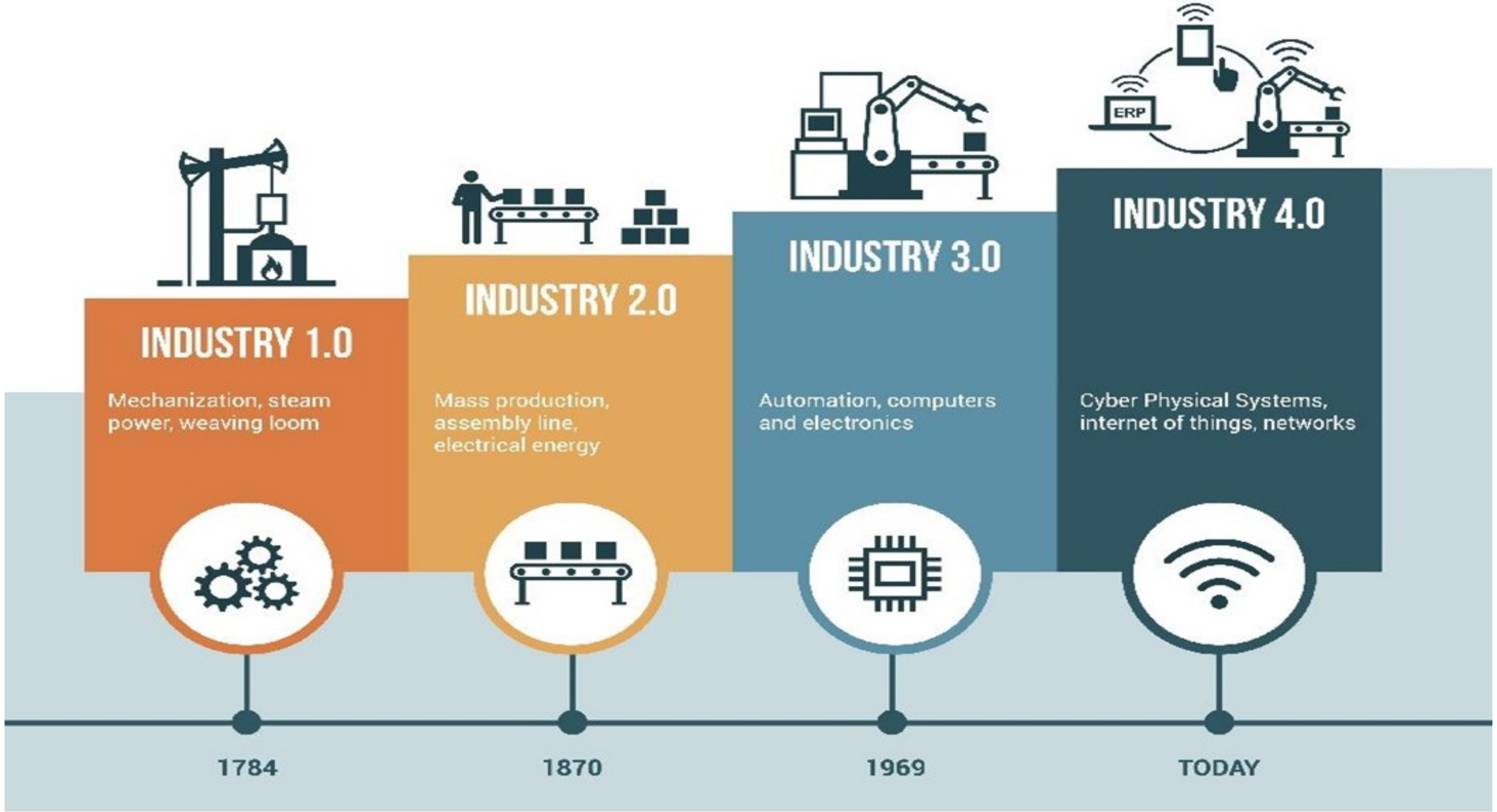
- Smart industrial management systems to be integrated with the Smart Grid, thereby enabling real-time energy optimization.

- Measurements, automated controls, plant optimization, health and safety management, and other functions provided by networked sensors.

- IIoT in manufacturing will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0.

- In the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate $12 trillion of global GDP by

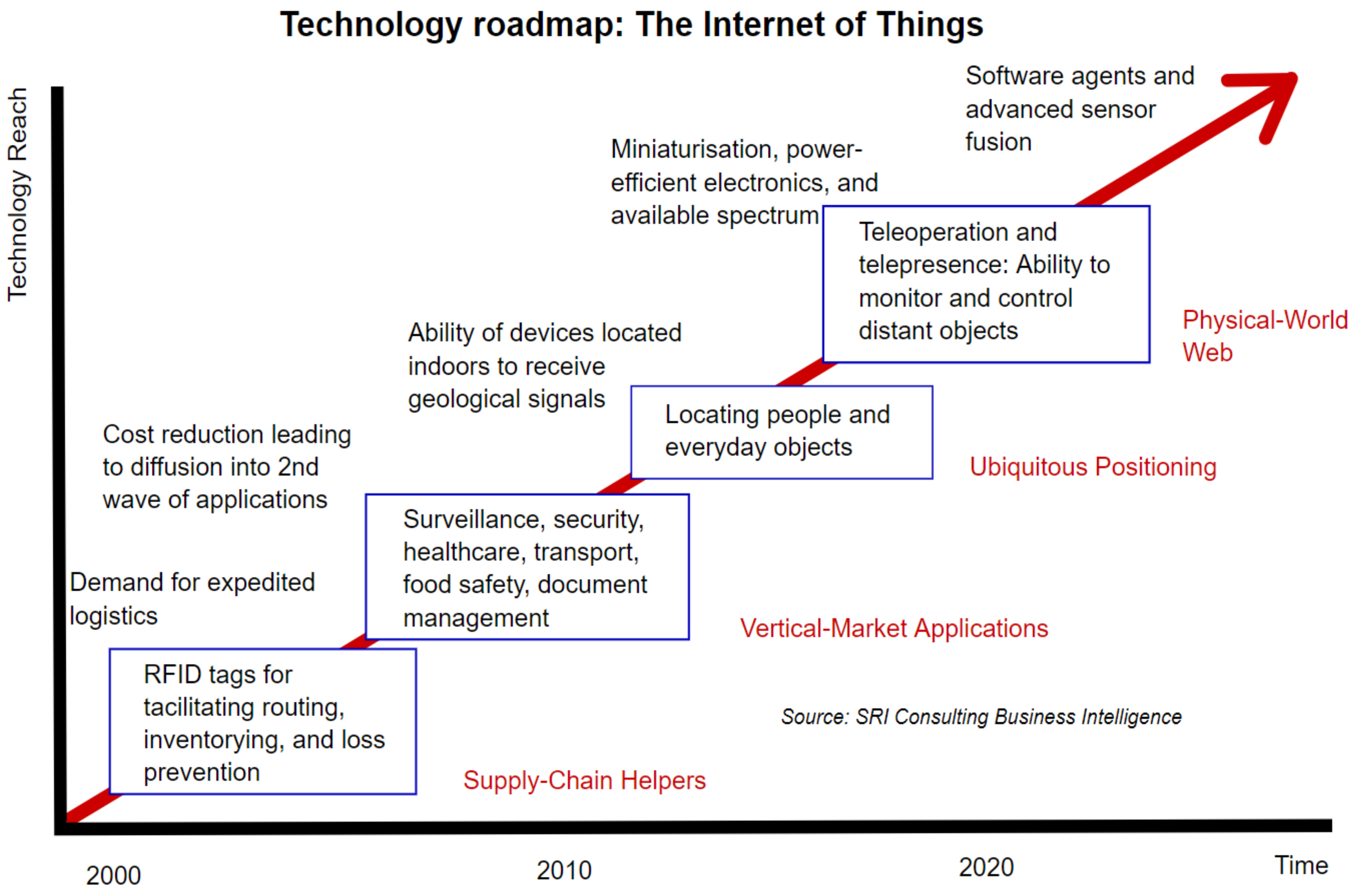
Industrial IoT


ERP
INDUSTRY 1.0
Mechanization, steam power, weaving loom
INDUSTRY 2.0
Mass production, assembly line, electrical energy
INDUSTRY 3.0
Automation, computers and electronics
INDUSTRY 4.0
Cyber Physical Systems, internet of things, networks
1784
1870
1969
TODAY

http://www.aberdeenessentials.com/opspro-essentials/industry-4-0-industrial-iot-manufacturing-sneak-peek/

Industry 4.0 is a name for the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing.

Technology Roadmap for IoT


Technology roadmap: The Internet of Things
Technology Reach
Software agents and advanced sensor fusion
Miniaturisation, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geological signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for tacilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
2000
2010
2020
Time

Source: SRI Consulting Business Intelligence

IoT Legal Aspects – Data Security and Liability

- The more connectivity you have, the less security you have” (Vice President of engineering at Threat Track Security Inc).
- As our world becomes more connected, it also becomes more susceptible to hacking and cyber attacks.
- Hacking a smart bulb
- Appropriate security measures must be implemented into IoT devices, in order to protect data from loss or any form of unlawful processing, but who is liable in case of a security failure?
    - The state?
    - Private security companies that are involved?
    - ISP companies?
    - The communication component manufacturer?
    - Maybe all of them?
- Possible solutions?
    - Contractual relationships – is obtaining consumer’s consent is enough?
    - Shared responsibility.

IoT Legal Aspects – Privacy

- IoT developments raise inherent privacy problems, because a main goal of these developments is to create and transfer many kinds of data – including personal data.
- Privacy problems in situations where a person obtains another's private data relating to:
  - Lighting devices – hours spent at home and away from home
  - Wearable devices – tracking locations and whereabouts
  - Medical devices – our health condition
  - Possible solutions?
  - Privacy by design
  - Consent (privacy policies)
  - Anonymizing the data
  - A "Notice and Takedown" mechanism?

IoT Legal Aspects – Intellectual Property

- In the case of IP rights, the main question is who owns the data that IoT devices create and send through the Internet. As mentioned above, this data is typically valuable for stakeholders, and therefore the IP ownership question arises.

http://www.ruthtrumpold.id.au/destech/?page_id=516

IoT Legal Aspects – Discrimination

- As data from IoT devices enables stakeholders to sort consumers more precisely than ever before, there is a concern that such sorting has the potential to turn relatively benign forms of organization and differentiation into new and invidious forms of discrimination. Particularly when coupled with Big Data or machine learning analysis, employers, insurers, lenders, and others may use data from IoT devices to make inferences and assumptions about individual consumers.
- Not only does decision-making have the potential to create troublesome yet invisible forms of economic discrimination, but it may also enable illegal discrimination against those in protected classes, such as race, age, or gender, based on misused IoT data.

ITU : I Thank U