ISOC PT
CNCS C-DAYS CONFERENCE
Coimbra, 21/Jun/2018

IOT Security and Privacy Agenda

AND SOME RESEARCH DIRECTIONS

Henrique Domingos, ISOC, FCT/UNL

Internet Society (ISOC)

www.isoc.org

Internet Society Portugal Chapter

IOT Security and Privacy Agenda

AND SOME RESEARCH DIRECTIONS

Henrique Domingos, ISOC, FCT/UNL

… “Yet Another” IoT (or IoE) Definition

- The Interconnection, via Internet (concretely via IP), of a new generation of heterogeneous computing devices with more or less processing power, memory and energy resources, embedded in a variety of everyday objects (not traditionally considered to be possible computers) enabling these objects to sense, process, actuate, send and receive data

- **What kind of Objects or Things ?**
  - **The Internet of Everything !**

IoT: News Words, New Concepts ?

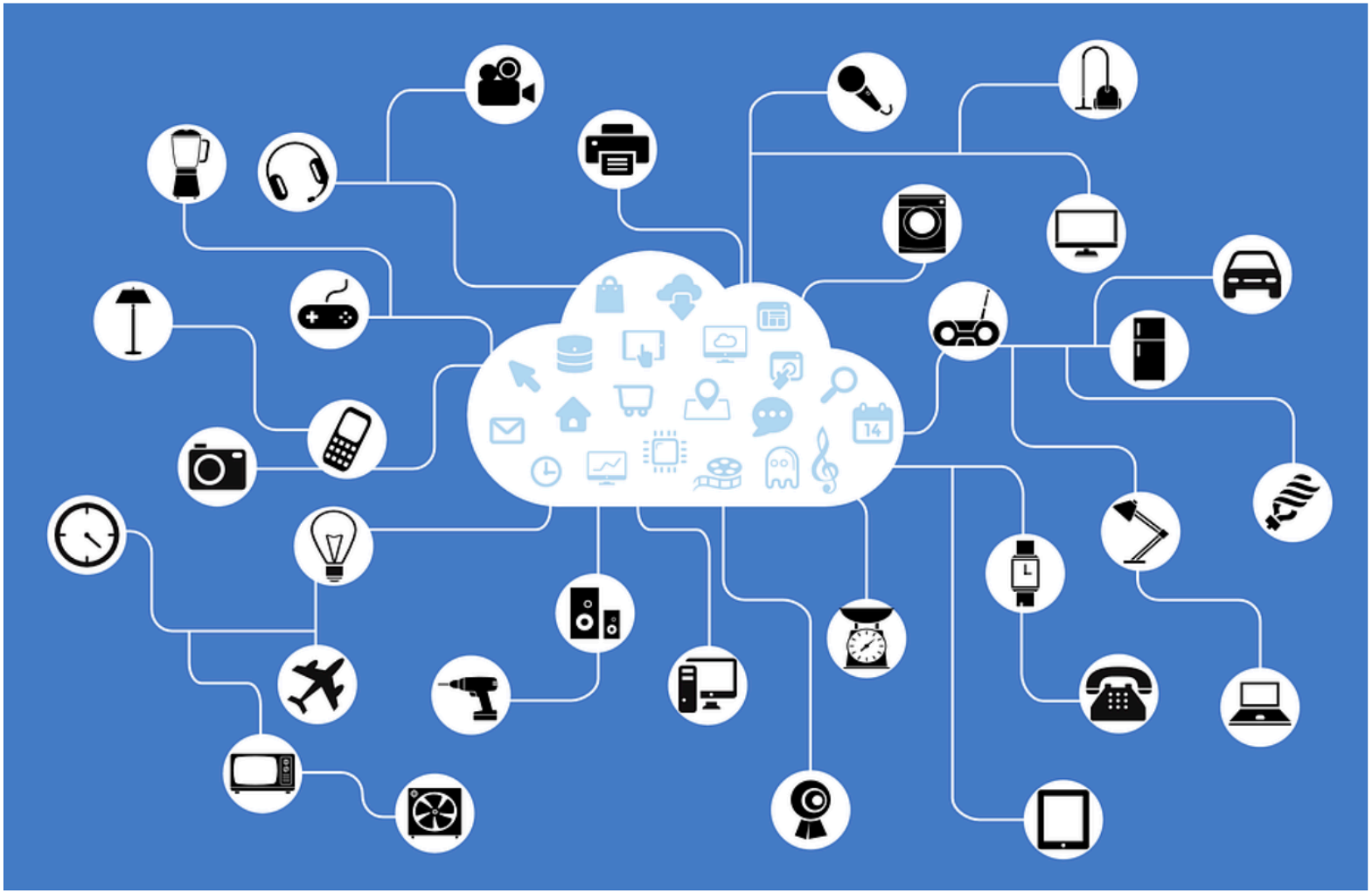
- Word invented in 1999 (related to RFID Tech)...
- ... But the idea comes from late 70's, in looking to IP as a way to interconnect "any IP enabled computerized device"
  - Early examples, late 70's: IP-enabled-toaster, drinking machines in university campus, etc…)
- **So is not so new … The magic *thing* here is: "The Internet Design Model and the "Amazing IP Design Principles for Scale"**

If IoT is not “new”
… why is now a “target of big interest ?

- Progressive widespread adoption of IP and IP Interoperability
- Maturity, mass-production and availability of data-link layer wireless tech (ZWAVE, ZIGBEE, POWERLINE, BT 4.X, IEEE802.11, BT-BLE, IEEE802.15.X, IPV6LowPan/radio-links)
- Rise of Cloud Storage and Cloud Computing (and PaaS / SaaS Models adopted by IoT Providers)
- Microelectronics, LSI and Miniaturization of micro-computers
- The raise of mobile and ubiquitous connectivity
- Computing Economics
- Advances in BIG Data Analytics and the rise of the value of “aggregated information”
- **TOGETHER WITH THE CONFLUENCE OF NEW MARKET TRENDS AND BUSINESS OPPORTUNITIES !**

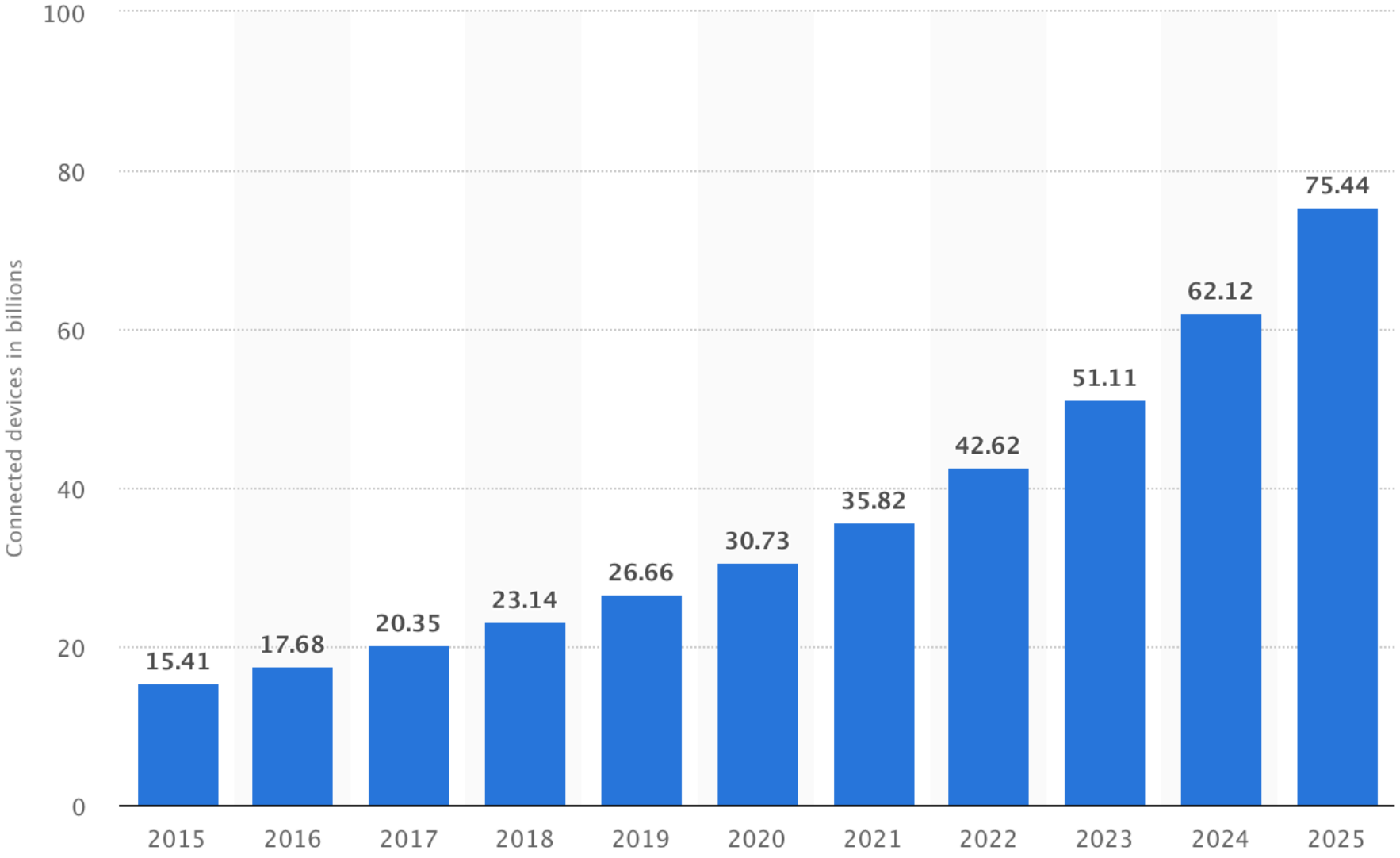
IoT Expansion: IoT > IoE (Internet of Everything)

STATISTA.COM

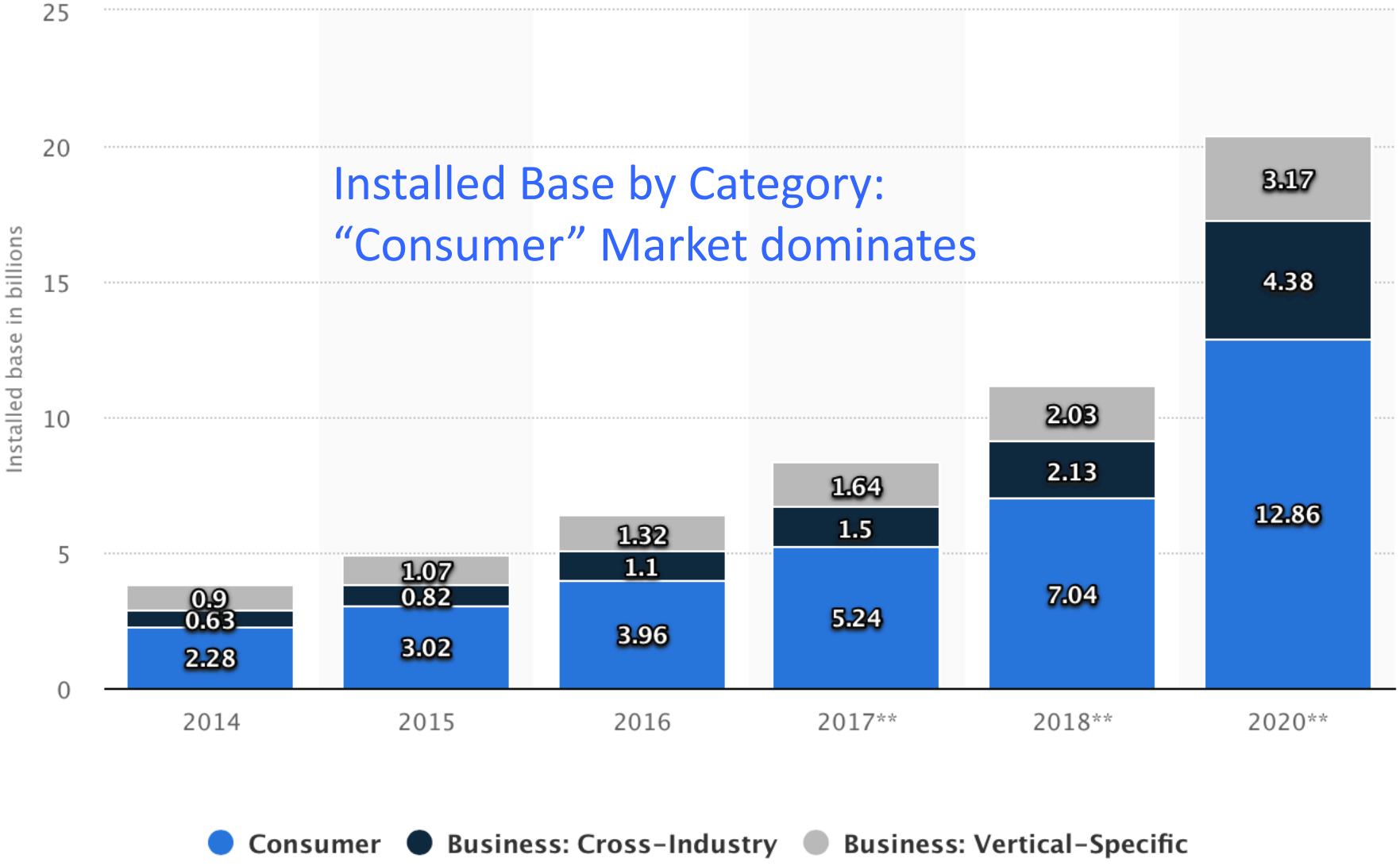


IoT Expansion: IoT > IoE (Internet of Everything)

STATISTA.COM



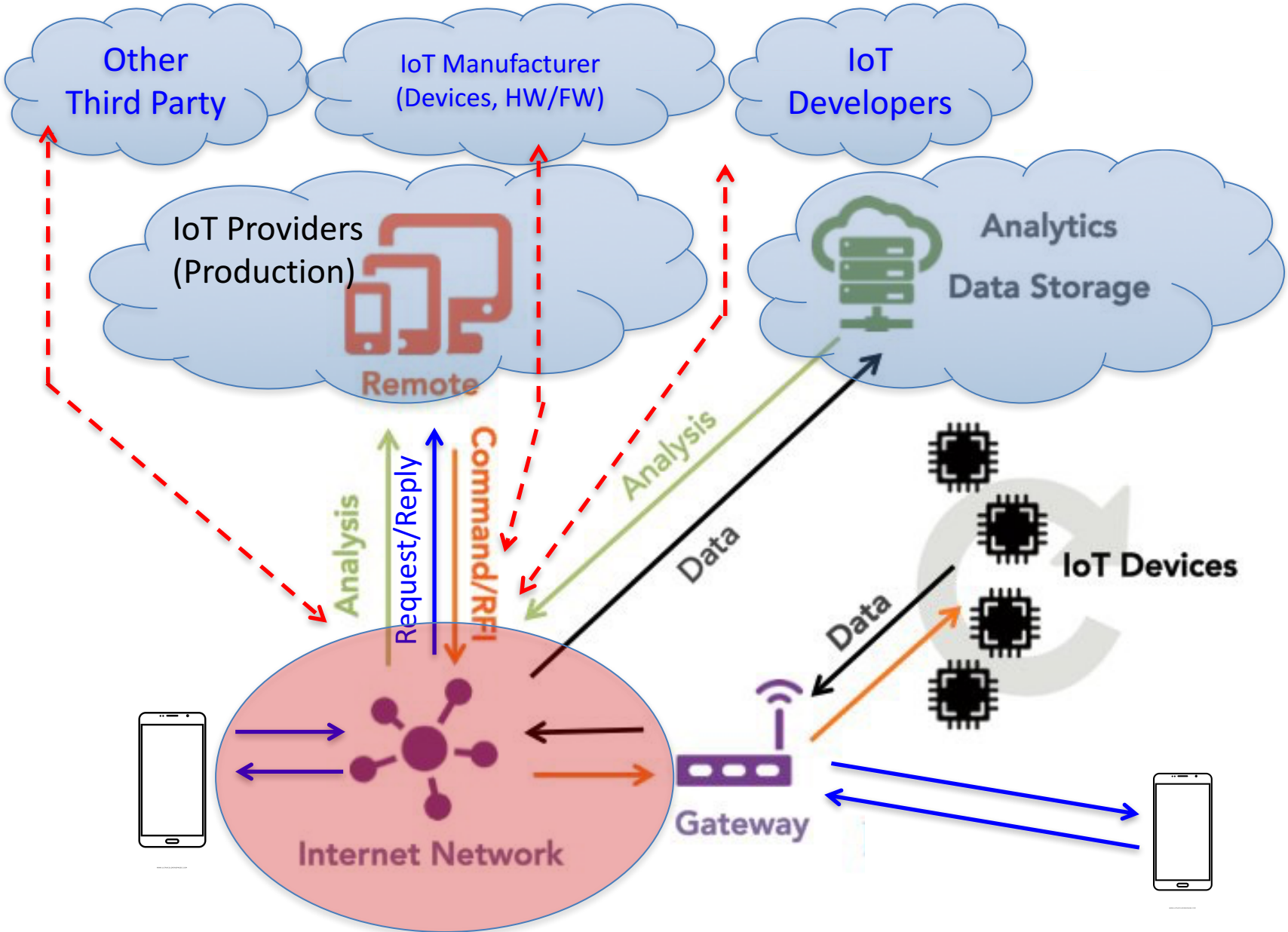
IoT Expansion: IoT > IoE (Internet of Everythong)



IoT Expansion in Multiple Sectors (Markets)

- Devices more and more widely used in:
  - Consumers in the personal space, homes and offices (~3 to ~7 B things from 2015 to 2018
  - … But it is now expanding to Healthcare Management Services, Cities, Factories, Farms, Industrial Plants, extended SCADA infrastructures, smart vehicles:
  - **MORE AND MORE CRITICAL ECO-SYSTEMS**
    - **SO FAR SO …. GOOD (perhaps): More Exigent Markets for RELIABILITY, TRUST, SECURITY AND PRIVACY ?**
  - **Different application domains … sharing (with more or less differences) the same architectural approaches and the same increasing concerns on reliability, trustability, security and privacy**

A Typical Architecture in a IoT Ecosystem



1st Take-Away IDEA

The Key-Drivers for a Successfully IoT are the same that are URGENT and RELEVANT for the INTERNET SUSTAINABILITY

The Key-Drivers for the Success of IoT

- IoT is the natural evolution of a Global Internet, as designed in its design principles
- IoT Ecosystems will be successfully if not addressed as “closed/isolated” islands
- IoT Success depends on the Global Internet Sustainability, following its amazing design principles and design model, and following a relevant set of key drivers (in the debate today !)

The vision of ISOC Key Drivers in the Debate for a sustainable Internet

Net Neutrality

Security and Privacy Reliability and Trust

Sustainability of the Open Internet Model

Human Rights, Ethics, Liability and Compliance

Mismatched GAPS ?

Contradictory Concerns, Interests and Priorities …. ?

Different Internet and now IoT Stakeholders

ISOC PT
CNCS C-DAYS CONFERENCE
Coimbra, 21/Jun/2018

ISOC Key Drivers for a Trusted IoT

The vision of ISOC Key Drivers for a “Trust” IoT

- **IoT Trust (Security and Privacy) “By Design”**
  - https://www.internetsociety.org/resources/doc/2018/iot-trust-by-design
- The need for a Commitment Agenda for All the Stackholders involved

See ISOC Documentation

See

IoT OTA - Online Trust Alliance

https://otalliance.org/initiatives/internet-things

Concerns for IoT Security and Privacy

- **The big target in the IoT market today are consumer devices for the personal IoT space** (and IoT Platforms for Smart Homes and Offices)

  - **Privacy Concerns**: What data is transmitted/sent by devices to whom and when … and what are the guarantees for no data-leakage conditions ?

  - **Security / DDoS Concerns**: An attractive eco-systems for attack vectors (using “things” as botnets’ elements) in large attack surfaces, against critical systems

2nd Take Away IDEA

There is a Need for a New Generation of IoT Platforms for Reliability, Trust, Security and Privacy “By Design”

NEW FOUNDATIONS FOR DEPENDABILITY MODELS and TECHNOLOGICAL SOLUTIONS for IoT PLATFORMS

> Big Opportunity Challenges for Research and Innovation, better addressing competitive factors (including TRUST ECONOMY !)

Example for IoT in the USER Space: Security and Privacy Criteria for IoT Smart Home Platforms

- **Threat Model Definition**
- **Security and Privacy Properties**

  = Correct and verifiable implementation

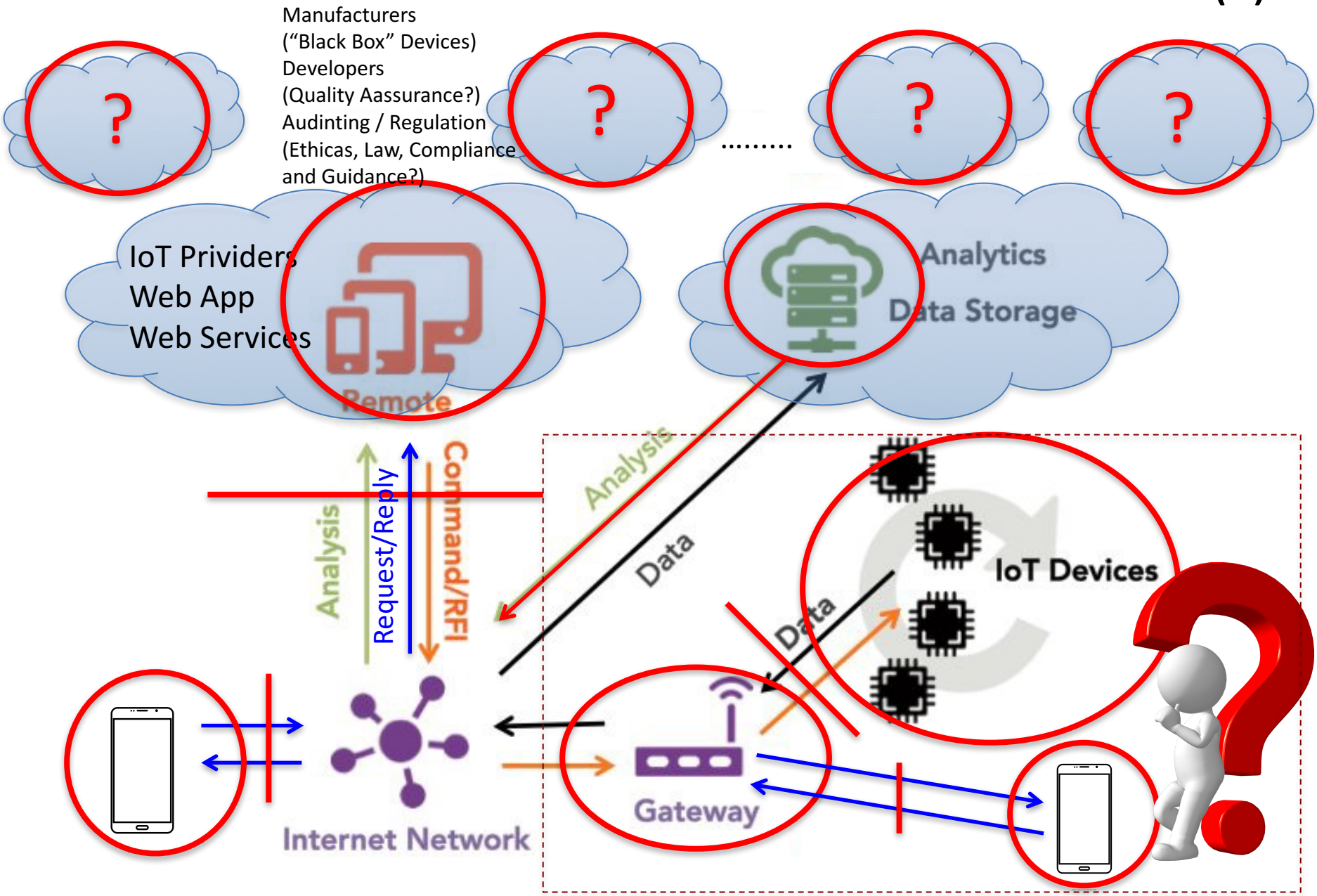
By Design

- … Complementarily (sake of sanity) we also need **Patching**

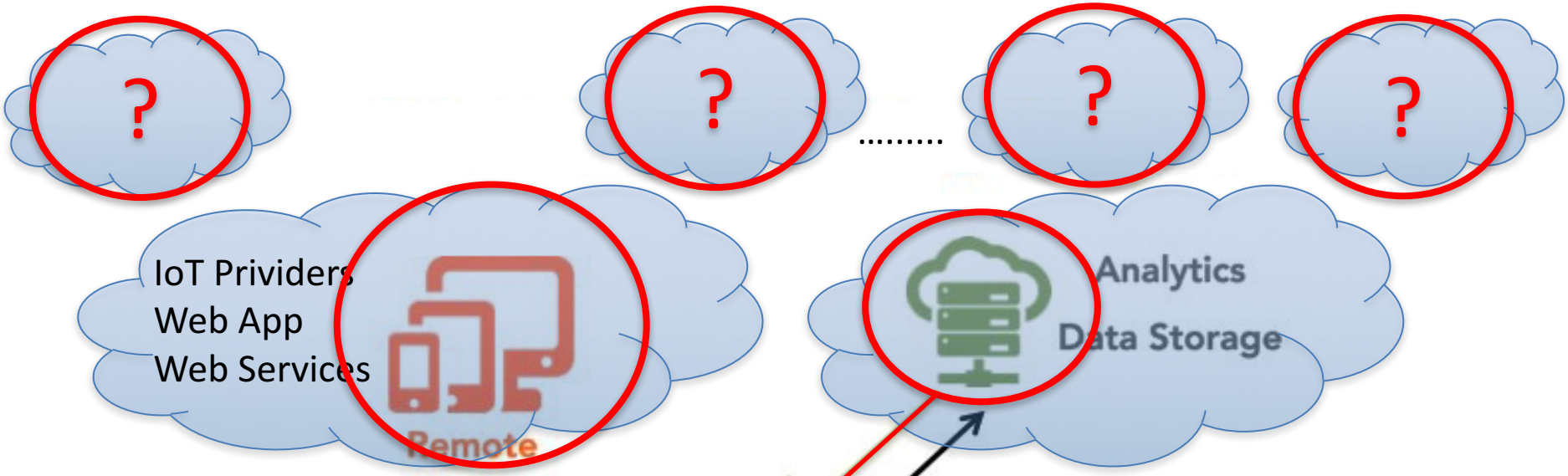
- But in many current IoT Tech, Security and Privacy is not not addressed BY DESIGN and not implemented at all !
- And lots of things ... Are not PATCHABLE !!!

SO HOUSTON ... WE HAVE A PROBLEM HERE !!!!

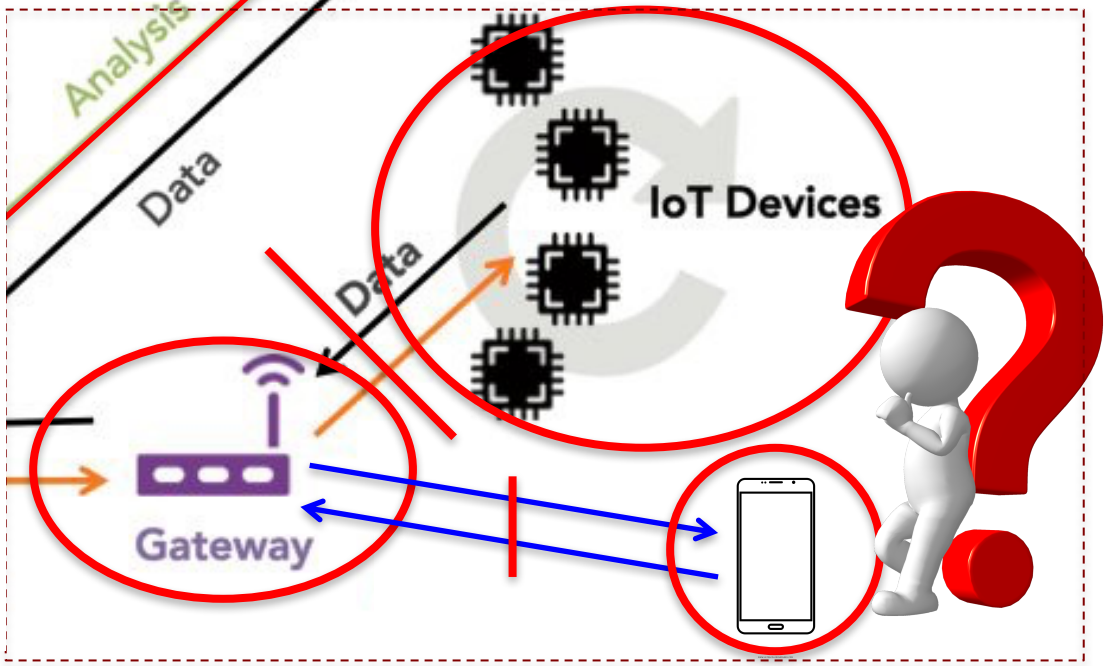
Different Attack Vectors in the IoT Attack Surface(s)



Different Attack Vectors in the IoT Attack Surface(s)



Manufacturers ?
("Black Box" Devices ?)
Developers ?
(Quality Assurance ?)
Auditing & Regulation ?
(Ethics, Law, Compliance and Guidance?)
Liability Model ?



Can we address the problem ? Is it Complex ?

- Challenge: Extension of the Attack Surface and the and the Different Implications and Correlations:
  - **Privacy Preserving CLOUD Services**
  - **Web Applications and Web Services**
  - **Mobile Apps and Mobile OSs**
  - **IoT Devices in their Specific Challenges**
  - **Different Interoperable Communication Substrates**
- And more specific issues on IOT Ecosystems and commitments of the multiple involved stakeholders

Agenda for a NEW GENERATION OF TRUSTWORTHY DEPENDABLE IoT PLATFORMS

RELIABILITY + AVAILABILITY + SAFETY + SECURITY + PRIVACY

… How to address from the CURRENT REALITY !??!

- Challenge: Extension of the Attack Surface and the and the Different Implications and Correlations:
  - **Privacy Preserving CLOUD Services**
  - **Web Applications and Web Services**
  - **Mobile Apps and Mobile OSs**
  - **IoT Devices in their Specific Challenges**
  - **Different Interoperable Communication Substrates**
- And more specific issues on IOT Ecosystems and commitments of the multiple involved stakeholders

Agenda for a NEW GENERATION OF TRUSTWORTHY DEPENDABLE IoT PLATFORMS

RELIABILITY + AVAILABILITY + SAFETY + SECURITY + PRIVACY

IoT Current Reality ☹

- **Poorly designed devices** (HW/FW), **No patching**
- **Users' Unawareness / Non liability** to the Users (as consumers)
  - "The problem of "Cheap Smart Things, Ready to Go"
  - … Fun, not critical … I don't care … But What if it is a TESLA ?
- **Lack of commitment, incentives and conjugated efforts of the multiple stackholders involved**: Devices' Manufacturers, IoT SPs
- **Closed Eco-Systems of Manufacturers and IoT Providers: Lack of Standardization, Vendor Lock-in Practices/Interests**
- **Hackers and Insider Attacks** / "Honest But Curious" Sys Admins, Privacy Breaks and Data Leackage (Cloud and IoT Service Providers)
- **No Intermediation**
- **Lack of Regulation / Guidelines / Quality Assurance / Compliance** Rules / Certification from Regulation Entities, Government

IoT insecurity or Io(untrustable)T

- Around ~20% of tested mobile apps by different entities) to control IoT devices did not use HTTTPS, TLS, IPSEC/SSH Transport or Tunneling Solutions to the Cloud
- Easily “Breakable Devices” (under the User Unawareness):
- Lots of devices not providing secure pairing with mutual authentication (Device-Device pairwising or Device- IoT routers or Devices- smart hubs)
- No encrypted communication between devices and routers/smart hubs: cleartext in the air !!! Anyone can “hear/see/feel” everything in our home …
- Replay attacks: injection of commands… => Inconsistent Device States (touch !!!)
- Cleartext IP payloads (data from/to Devices) sent though IoT(Smart?)Hubs to Cloud-Services.
- No password enforcements, weak (easily breakable) passwords
- Many IoT Routers/Switches/Smart Hubs are easily hacked (ex., IoT Hackiong Tools/Toolkits/… Commercially Available for Eveyone !!!)

IoT insecurity or Io(untrustable)T

- Not Protected TFTP/UDP/IP for Firmware Updating … Weak Injection of Firmware (ARP Poisoning Attacks + Fake HTTP Repositories)
- Most of the IoT services did not provide authenticated/encrypted firmware updates, if updates were provided at all
- Some IoT cloud interfaces did not support two-factor authentication (2FA)

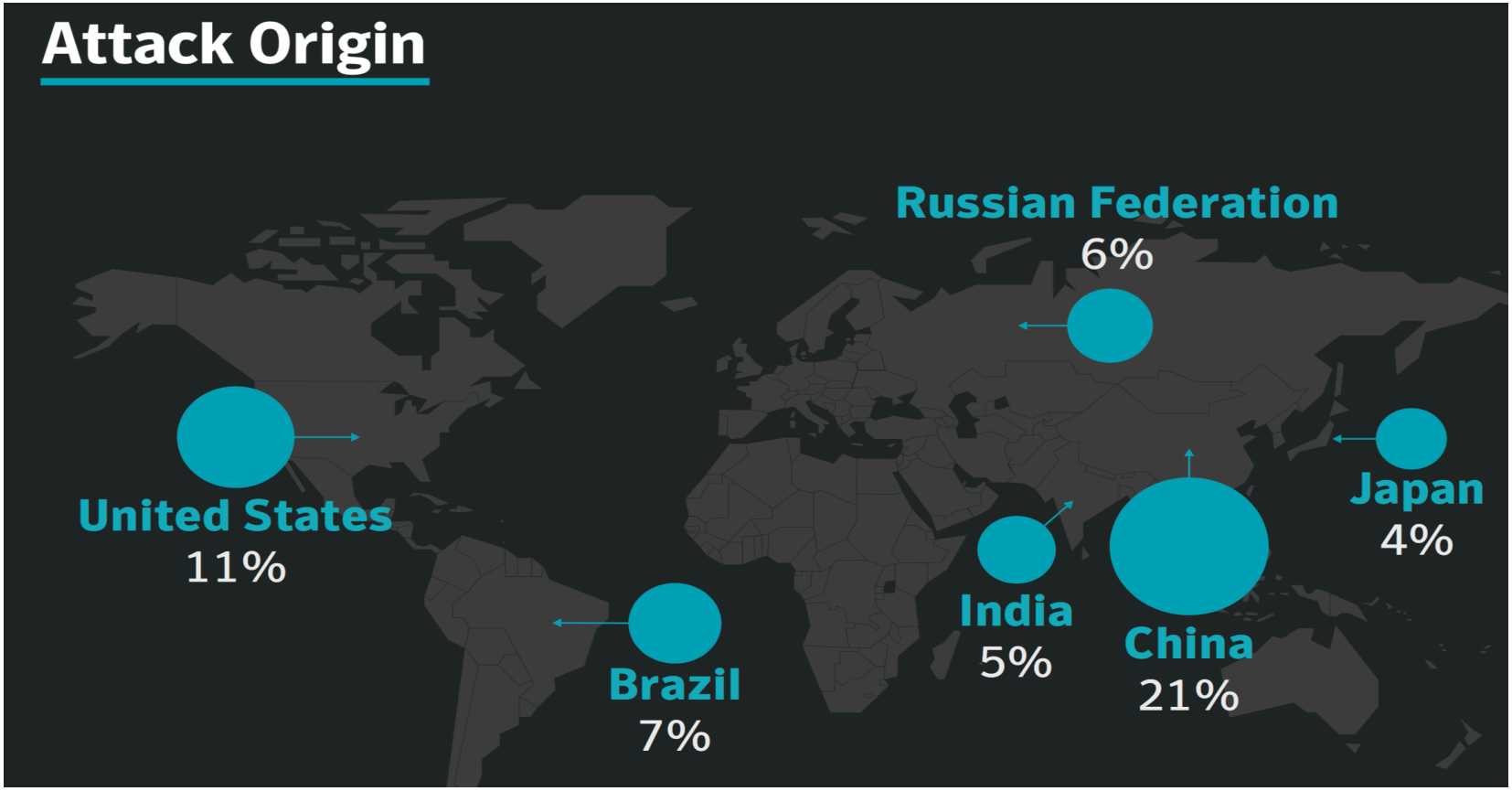
  use HTTP !!! Or Even when HTTPS is used .... (WEAK TLS Behind !: SSL1, SSL2, SSL3, ...)
- Many IoT services did not have lock-out or delaying measures to protect users' accounts against brute-force attacks
- Some devices did not implement protections against account harvesting
- Many of the IoT cloud platforms included common and well-known web application vulnerabilities (ex., OWASP Top Ten Vulnerabilities)

3rd Take Away IDEA

The Problem is URGENT !

IoT Attacks, 2016-2017-…

- **600% increase** in attacks against different IoT devices, all over the world …



Symantec Security Threat Report, 2018

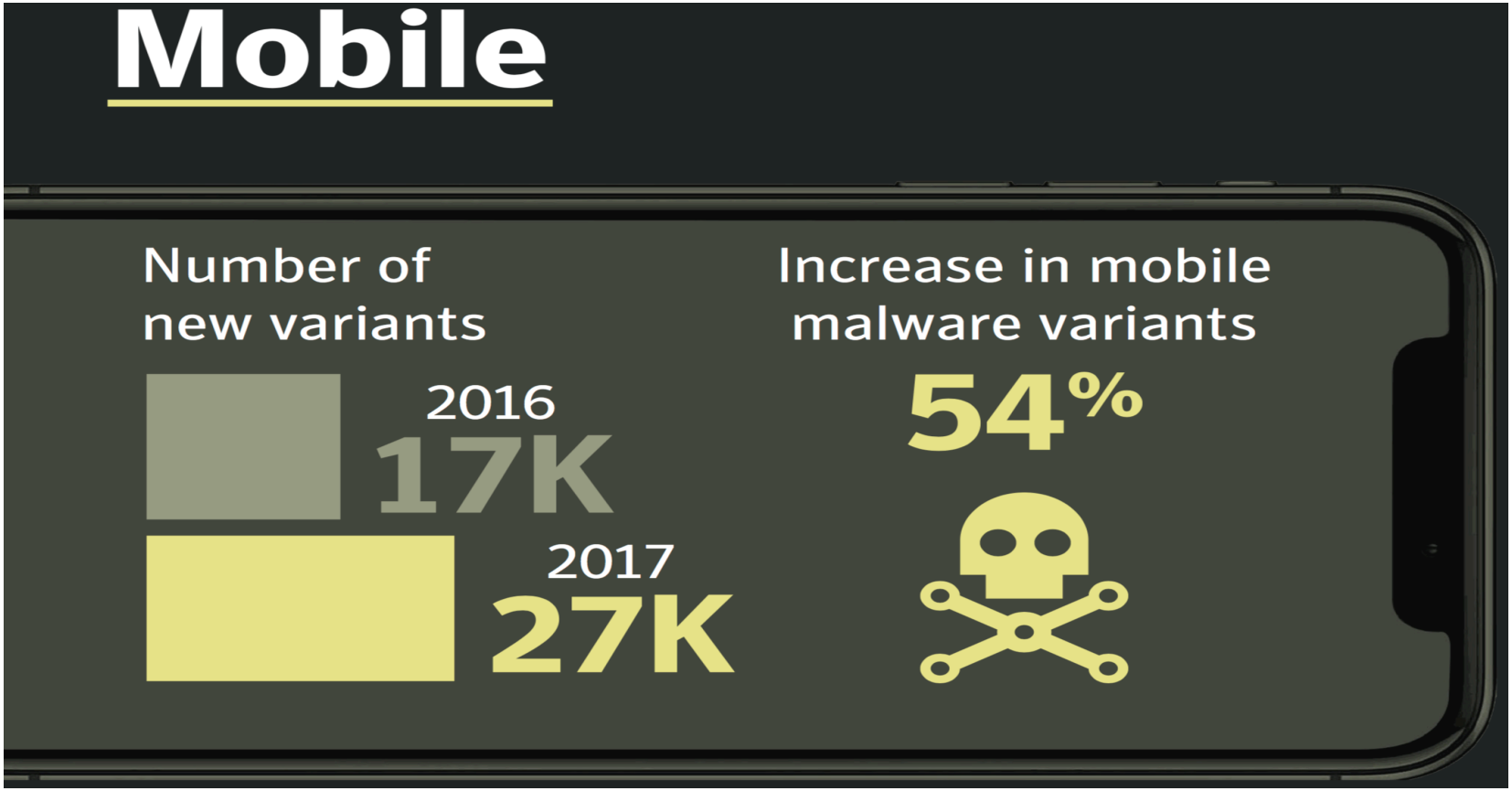
The IoT Insecurity Landscape

- **IoT attacks will likely diversify as attackers seek new types of devices to add to botnets**
- During 2016:
  - the impact of attacks due to the **Mirai botnet** caused a serious disruption with large DDoS attacks.
  - Many Cybersecurity Professionals agree that Mirai Changed Completely Their Perceptions About IoT Device Threats
- Many attacks are focused on routers and modems, as well as on “malware” / Unsecure Apps and in using infected devices and routers (or smart hubs) to power botnets.

- RISKS = VULBERABILITIES x THREATS’ PPOTENTIAL
- Amplification Factors: The different Attack SUrfaces

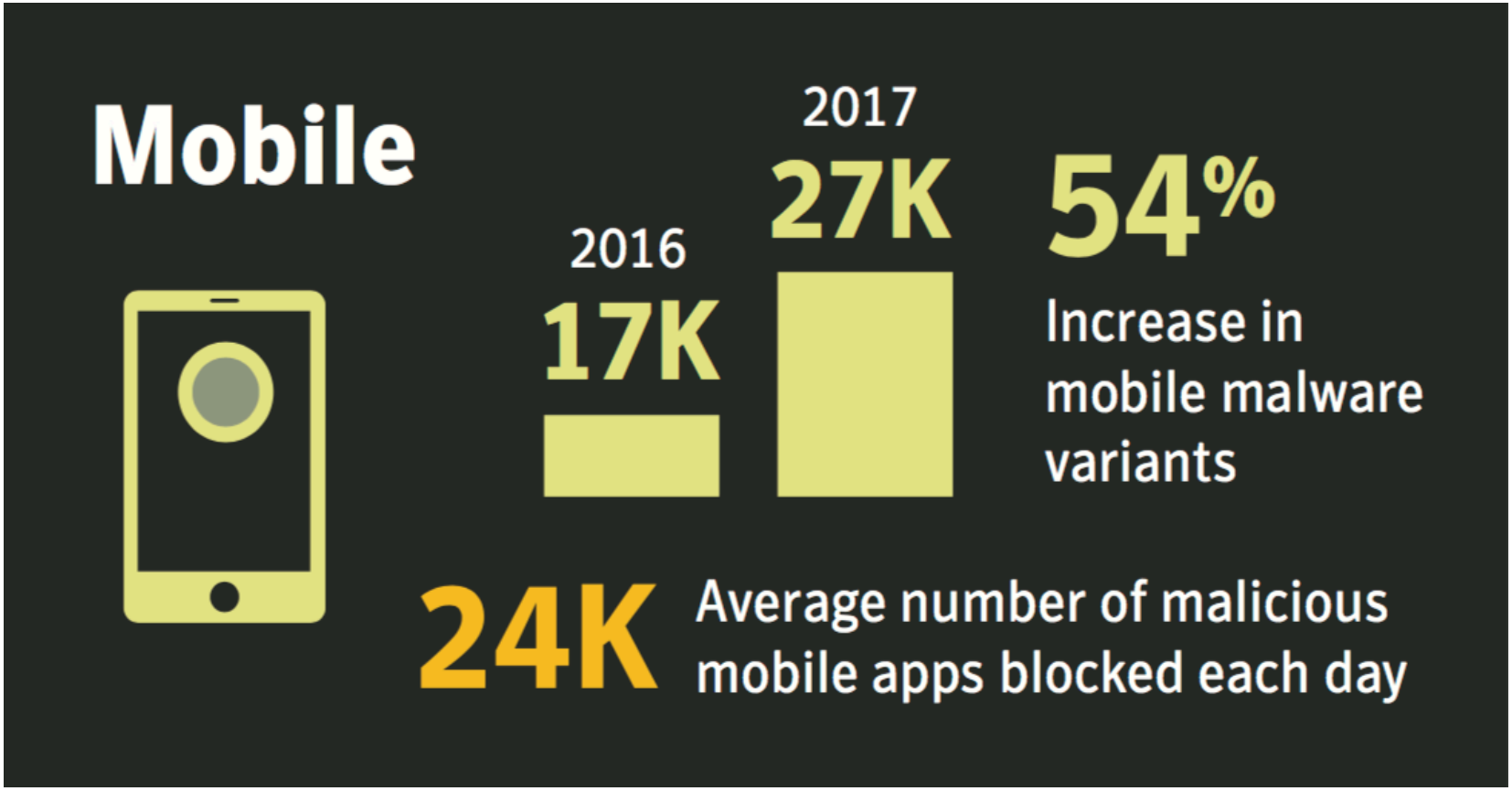
Example of Amplification Effect

IoT x Mobile Apps in the “BYOD” Paradigm



Symantec Security Threat Report, 2018

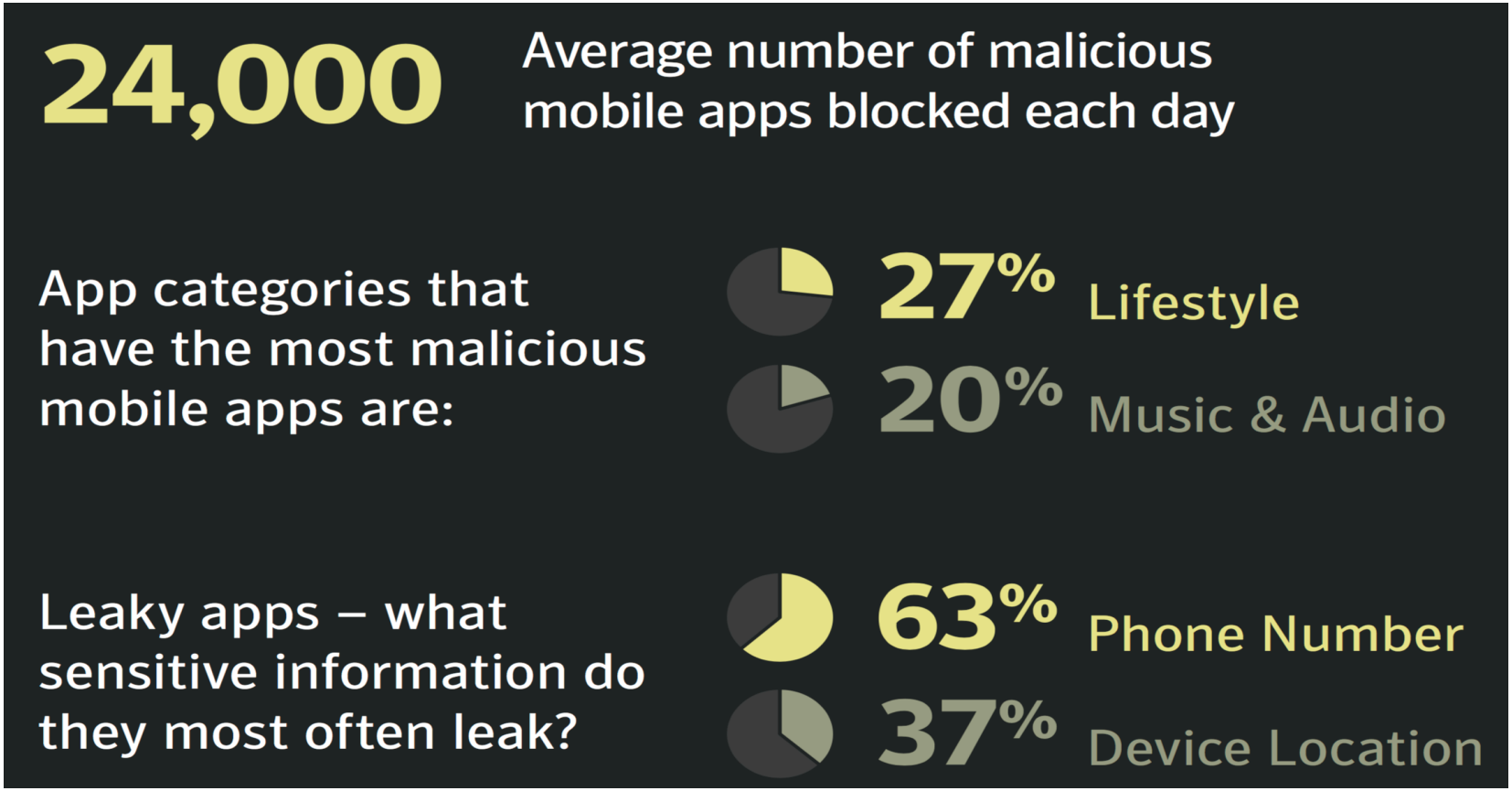
IoT vs. Mobile Apps



Symantec Security Threat Report, 2018

IoT vs. Mobile Apps

- Mobile and Ubiquotous Computing Vulnerabilities as an Amplification Effect



Symantec Security Threat Report, 2018

4rd Take Away

The Agenda for R&D on IoT Platforms …

Challenges and Contributions in the R&D Community ? Some Ideas and Example of OnGoing Work

- IoT Platforms and the new Generation of Smart Vehicules
- Research Lines for IoT Security and Privacy Solutions

Conclusions

1. The IoT Success will depend on the current debate on the **Key Drivers for a Sustainable Internet** as an Open Global Internet for Everybody ! (**See the ISOC/OTA Concerns !!!**)

2. IoT Security and Privacy requires **collaboration and commitment across a wide range of stakeholders**

3. Relevant directions for an **Urgent Agenda for IoT Trusted Platforms "By Design" requiring Privacy Control and Data Management Research** (devices, smart hubs, and issues related to the various Ecosystems)

4. Opportunity for R&D in proposing **Better, Trust and Privacy-Aware Innovative Privacy-Enabled IoT Platforms**

End-To-End Security and Privacy Arguments (in Systems' Design !)