The Internet of Things

Niels Olof Bouvin

Overview

- **What is the Internet of Things?**
- The vision
- Domains of the Internet of Things
- The challenges
- RFID

What is the Internet of Things?

- (CERP-IoT 2009): *"Internet of Things (IoT) is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual* **'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.** *In the IoT, 'things' are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information 'sensed' about the environment, while reacting autonomously to the 'real/physical world' events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these 'smart things' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues."*

Many definitions for IoT

- **The link between the real and the digital world**
- **Machines talking to machines (M2M)**
- **Everyone and everything connected via the Internet**
- ***The Internet of Things is a system of physical objects that can be discovered, monitored, controlled, or interacted with by electronic devices that communicate over various networking interfaces and eventually can be connected to the wider internet.*** **[Guinard & Trifa, eds.]**

Constituent parts of the Internet of Things

- Identity
- Connectivity
- Capability

Identity

- **Primary requirement**
- **Scannable ID, e.g., RFID, barcode, QR-code, etc**
  - cheap, often limited, "dumb" objects
- **Inherent ID, e.g., MAC address (WiFi, Bluetooth LE, etc), assigned identity**
  - more expensive, more capable, "smart" objects

Connectivity

- How can we address the object?
- IR, Bluetooth (LE), Zigbee, WiFi, etc.
- Internet Protocol, or more specialised protocols (for resource constrained devices)

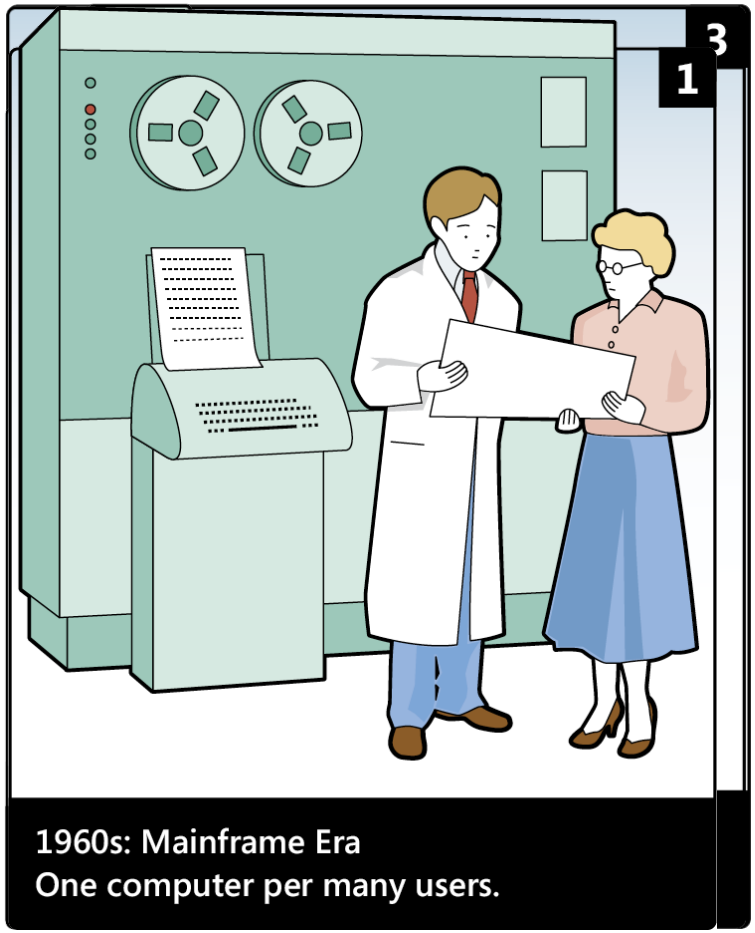
Capability

- What can the object *do*?
- Simple: Identification
- Intermediate: Sensing
- Advanced: Reacting

Overview

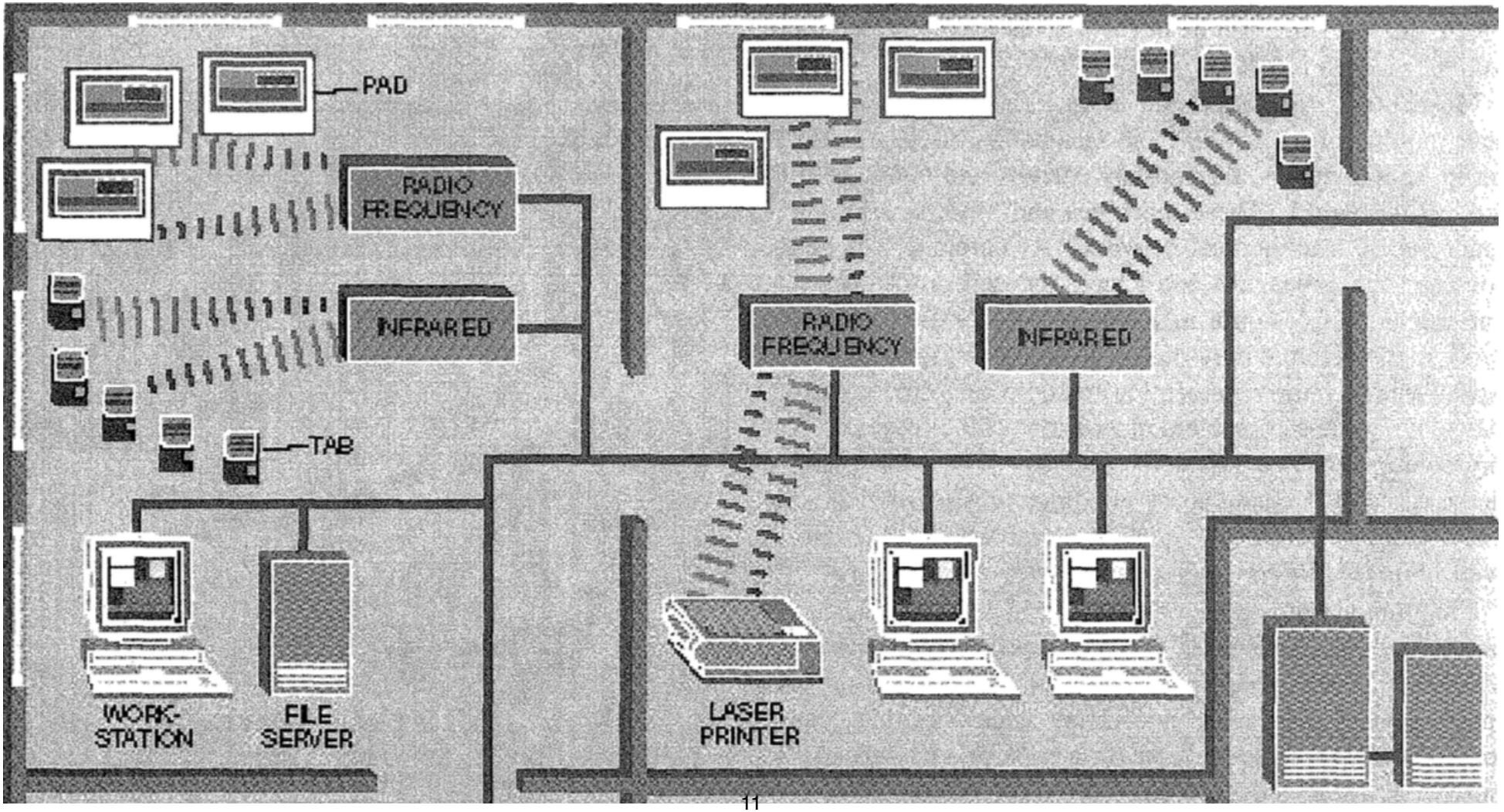
- What is the Internet of Things?
- **The vision**
- **Domains of the Internet of Things**
- **The challenges**
- **RFID**

Towards the Internet of Things



Visions for the Internet of Things

- **Mark Weiser: The computer for the 21st century**
  - a paper that would herald what came to be known as "pervasive computing"



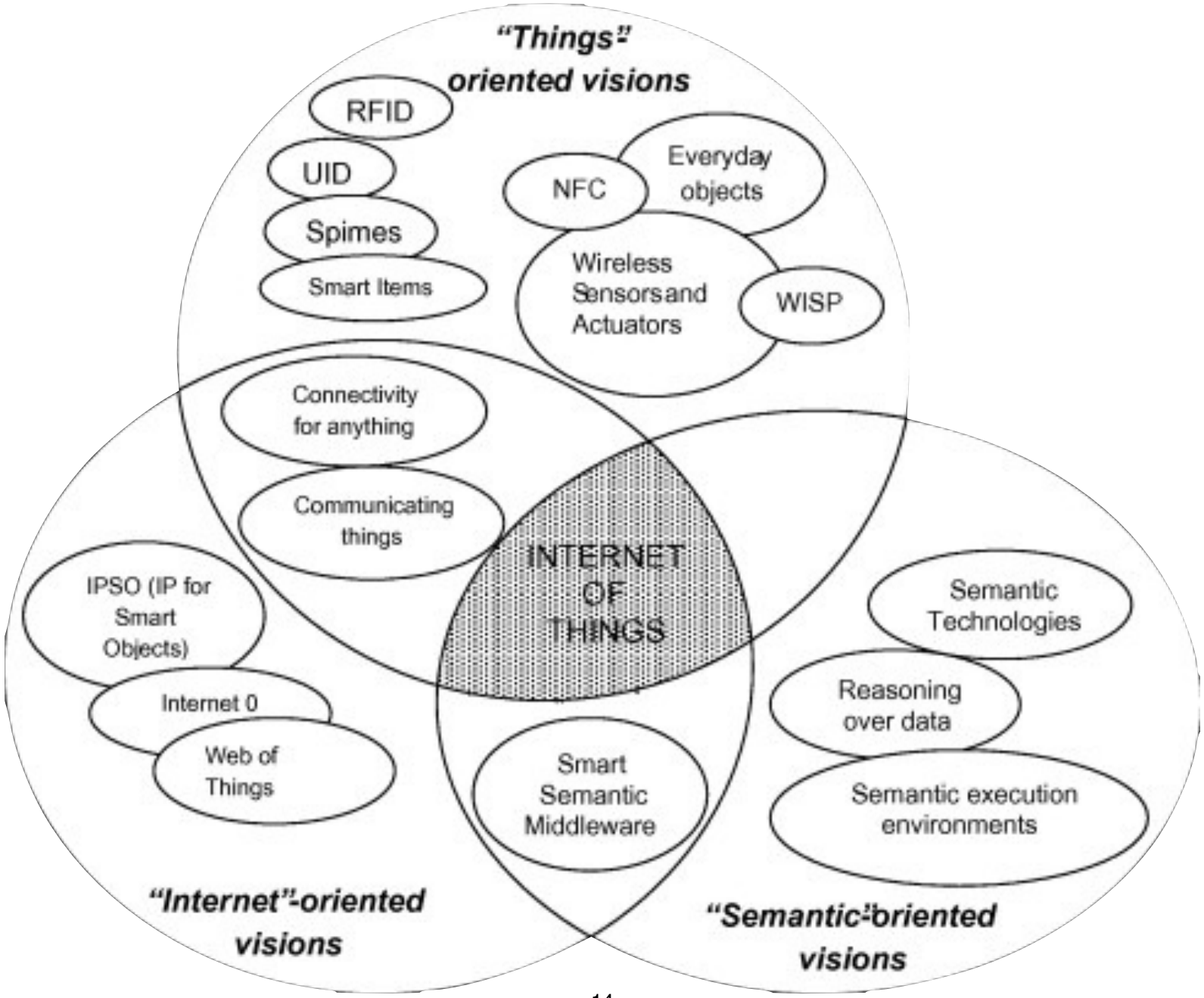
The early days of the Internet of Things

- **Motivated by caffeine and sloth…**
- **CMU Coke Machine**
  - CMU CS Department, U.S.A.,1982- (several iterations)
- **The Trojan Room Coffee Pot Camera**
  - Computer Science Lab, University of Cambridge, U.K. 1991-2001

Microsoft SPOT

- **Microsoft Smart Watch SPOT 2004-8**
  - Smart Personal Objects Technology
  - general platform—watches **and** coffeemakers
  - data broadcast over FM band in USA (DirectBand—12Kb/s)
  - watches from Swatch, Suunto, Tissot, and Fossil
  - data feed subscription based ($60/year)

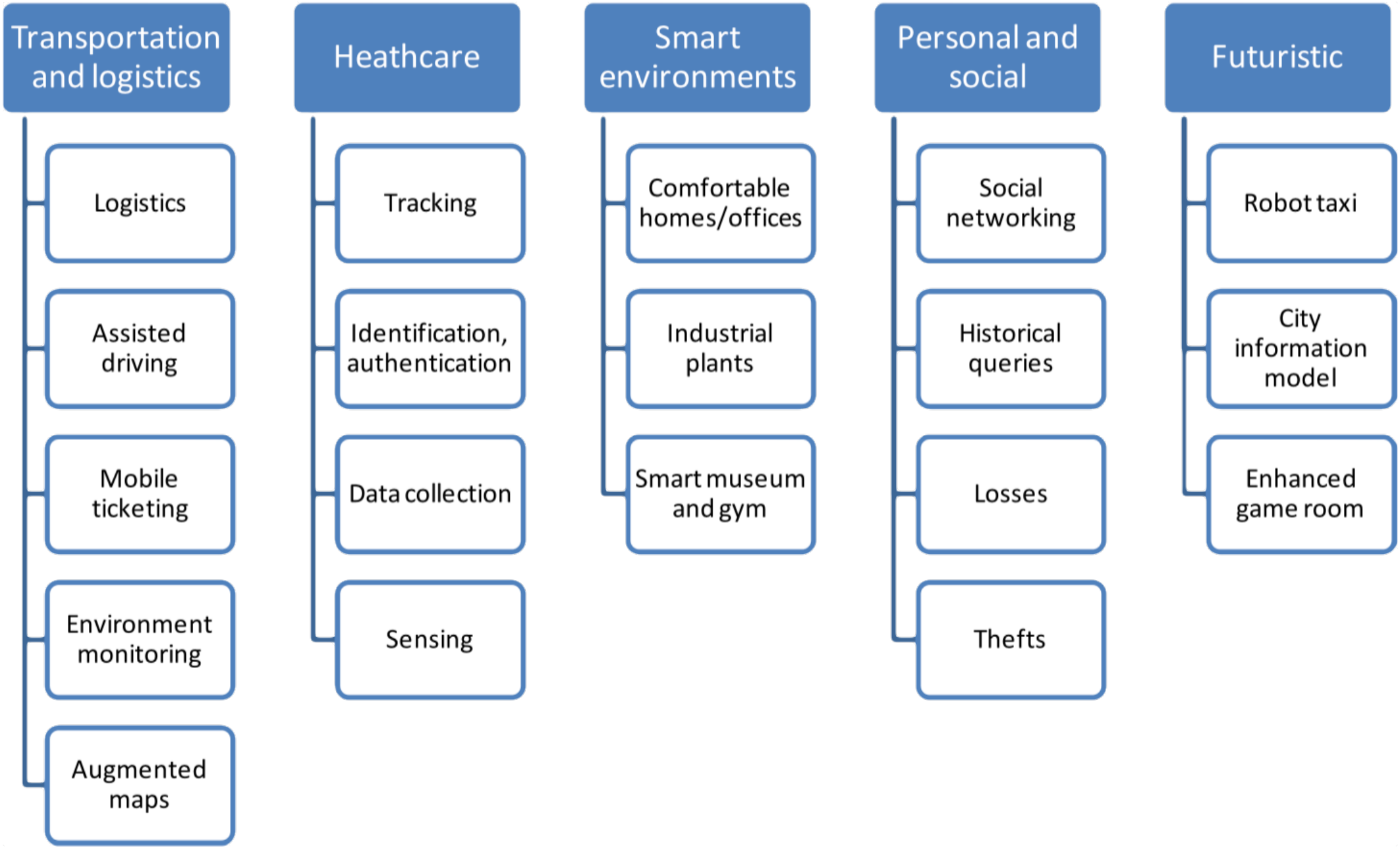
The Internet of Things: at the crossroads



Overview

- What is the Internet of Things?
- The vision
- **Domains of the Internet of Things**
- **The challenges**
- **RFID**

The Internet of Things: domains



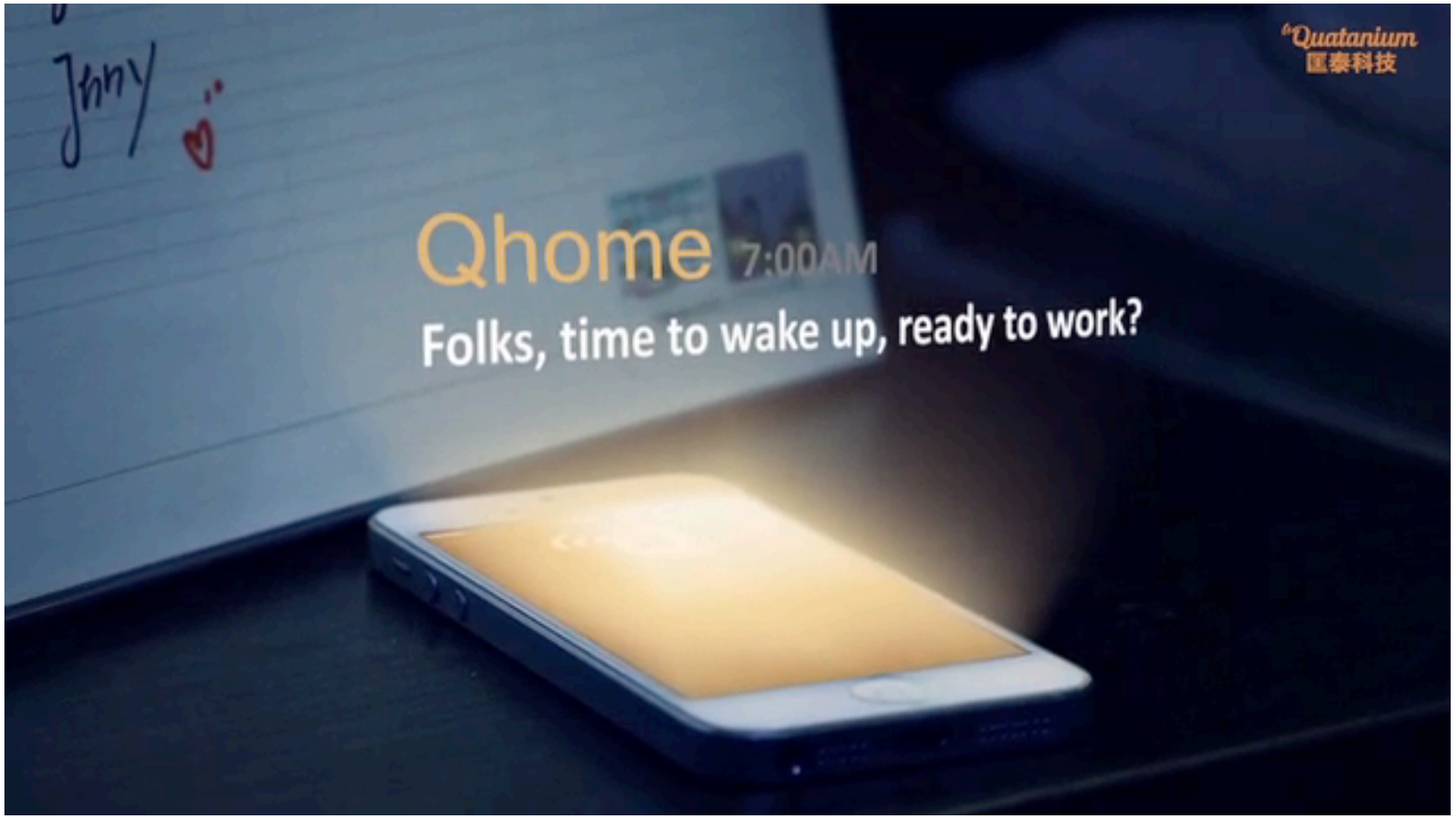
Logistics and supply chain

- **Precise tracking within and across organisations**
- **Shipping and transportation**
- **Manufacturing**
  - asset tracking: precise knowledge of components, both being ordered and delivered from suppliers, and on the shop floor
- **Post manufacturing**
  - delivery to customer
  - precise knowledge of constituent parts, their origins, and histories
  - monitoring of product during its lifetime to ensure quality and proper disposal

Home automation/Smart home

- **Smart metering**
  - electricity, water, heat
  - benefit in a fluctuating energy market
- **Home control**
  - builtin, or through after-market add-ons
- **Home surveillance**
  - fire, water leakage, intruders

QHome


Quatanium
匡泰科技
Qhome 7:00AM
Folks, time to wake up, ready to work?

Healthcare

- **Sensors, wearable or otherwise, enabling high fidelity surveillance of the sick, the injured, and the elderly**
  - detecting things, before they become an issue
  - enabling patients to live normal lives away from hospitals, yet still monitored
  - automated systems alerting patients without the need for a doctor
- **Tracking doctors, nurses, orderlies, patients, medicine, and equipment to ensure efficient and correct procedures at hospitals**
  - decrease dangerous or costly mistakes

The quantifiable life

- Keeping track of caloric intake, weight, exercise, sleep, etc, etc
- Wearable sensors (exercise monitors, smart watches)
- Mobile phones (GPS, accelerometers, …)

Wearables

- **Smart watches and other devices**
- **Always available, continually sensing**
- **Typically, small interface connected to smartphone gateway**
  - conserves battery, provides richer interface on larger device
- **Modern examples**
  - Pebble Watch; Apple Watch ; Google Wear; Samsung Gear
  - The Dash headphones
  - Fitbit, and other fitness trackers

Wireless Sensor Networks

- **Underlying many scenarios, many sensors distributed in an area monitoring and measuring the environment, digital or physical**
  - RFID tags, Bluetooth IDs, . . .
  - temperature, humidity, vibration,. . .
- **Zero (or very low) configuration, self-organising network**

Smart infrastructure

- **Smart Grid**
  - aligning production and consumption of electricity
  - across borders
  - especially crucial with renewable energy sources
- **Support for planning and living**
  - Smart Cities
  - traffic analysis based on crowd-sourced sensing
  - improved real-time data for commuters
- **Transportation**
  - fleet management
  - self-driving cars, etc.

Overview

- What is the Internet of Things?
- The vision
- Domains of the Internet of Things
- **The challenges**
- **RFID**

Challenges for the Internet of Things

- **The Internet of Things has many forms, many domains, and many associated challenges**
  - technological as well as legal and social

Energy usage and scavenging

- **A sensor with no power is no good**
- **Energy conservation**
  - long-lived batteries; highly frugal devices; low-energy networking and routing
- **Energy capture**
  - through radio signals (e.g., passive RFID)
  - through induction, photovoltaic, motion, . . .

Too many devices, too few IP addresses

- **We have nearly run out of (IPv4) IP-addresses**
  - 32-bit addresses seemed/was big enough 40 years ago. Today? Not so much
  - $2^{32} = 4.294.967.296$
- **Interim solution: use gateways to "hide" devices**
- **IPv6 to the rescue!**
  - 128-bit address space: We are not going to run out of IP-addresses anytime soon
  - $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
  - Transition painful, tedious, expensive, necessary, and taking place
- **6LoWPAN**
  - IPv6 over Low power Wireless Personal Area Networks

Naming and discovery

- IPv6 may address unique identities (10^{38} is **big**), but that is not enough:
- How are devices found?
- How are they named?
- How are their abilities discovered?
- How is interoperability ensured?

Standards, rather than standardisation

- **The Internet of Things is seen (perhaps rightly so) as a huge future growth opportunity across many fields**
  - to hold the keys to that growth is highly desirable
- **Result: Major players (Microsoft, Google, Intel, Apple, Samsung, Qualcomm, ARM, TI, etc.) present their own vision, tools, and systems**
  - promising startups are being bought by big companies (e.g., Nest acquired by Google)
  - small companies are interested in interoperability, big companies often less so
- **So far, no one solution dominant enough to force *de facto* adherence**
  - will this be a case for market forces or international agreements?

Data silos

- **Pre-Web Internet**
  - data flowed evenly across the hosts
- **Present Internet**
  - data flows from content providers to end-users; data about habits collected
- **Future (IoT) Internet**
  - countless sensors and devices streaming data towards central repositories (ie., clouds)
- **If major players succeed in creating dominant standards and systems, the collected data will end up on their servers**
  - which, presumably, is *the whole point* of playing for some of them. . .

Security and privacy

- **If I generate data, surely that data is mine?**
  - or is it? Better read up on the fine print in that EULA…
  - even if it *is* mine, where is it stored? How securely is it stored?
- **If my home, or the infrastructure I depend on, is "smart", it is also hackable and vulnerable**
  - security becomes a paramount concern
  - smart devices become potential vectors of attack
  - smaller devices cannot implement sophisticated security
  - smart grids must be protected at a high national and international level
- **Industrial espionage and sabotage**
  - stuxnet and its heirs

Summary

- **The Internet of Things is characterised by**
  - identity, connectivity, and capability
- **It posits a huge set of different devices collaborating and coexisting, collecting and correlating data**
- **The technical challenges are significant, as are the social and legal ones**
- **Who will hold the keys to the IoT? Will we see a balkanisation of systems, a centralisation, or is there a third way?**