ARM IoT Research Challenges

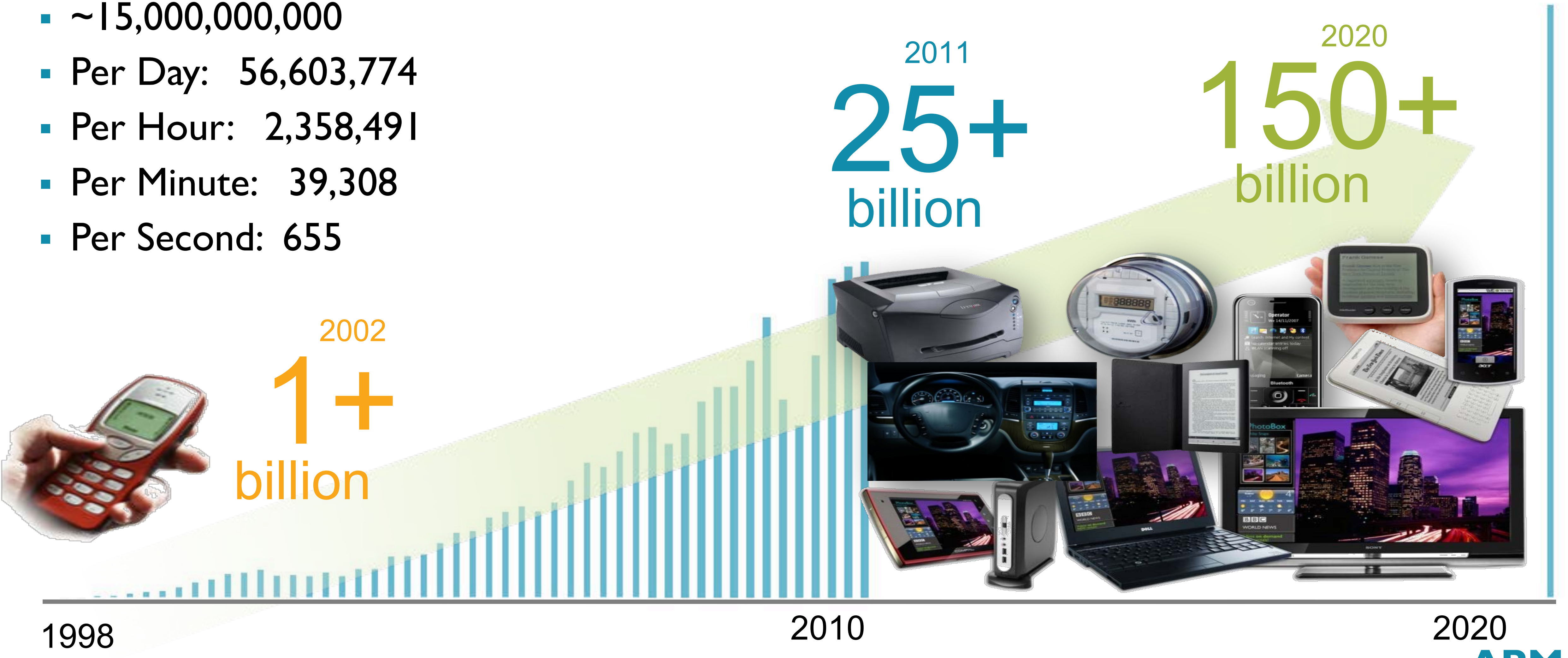
ARM

Dr John Goodenough
VP Technology & Collaboration
ARM Research
john.goodenough@arm.com

Edinburgh University Informatics Workshop
3rd July 2017

Q&A

- How many ARM cores shipped in 2015?
- ~15,000,000,000
- Per Day: 56,603,774
- Per Hour: 2,358,491
- Per Minute: 39,308
- Per Second: 655



ARM

IoT Security: A journey through standardization

ARM

Hannes Tschofenig

Edingburgh
03/07/2017

IoT security is a problem, according to media.

Top 5 IoT device security vulnerabilities

1. No or limited software update mechanism
2. Missing key management
3. Inappropriate access control
4. Missing communication security
5. Vulnerability to physical attacks

Our approach

- Make embedded development more friendly
- Use off-the-shelf Internet security protocols.
- Developed solutions in
  - Hardware
  - OS
  - Device Management / Communication security protocols

TLS/DTLS

- Most popular communication security protocol
- TLS for connection-oriented transports; DTLS for connection-less transports
- 1.2 is the most recent, finalized version
  - ~25 extensions
  - ~340 ciphersuites

- Has been difficult to "phase-out" old TLS versions and old crypto

TLS 1.3

- 1.3 in development since April 2014

- Supposed to an evolutionary development addressing security problems emerged with earlier specifications.

ARM

mbed TLS

- Our implementation of TLS/DTLS for embedded devices
- Open source with an Apache 2 license
- Modular design for optimizations and integration of hardware (e.g., new memory allocator, RNG, AES and ECC hardware acceleration)
- Code: https://github.com/ARMmbed/mbedtls

Standardizing TLS

- There are a few rules in the IETF:
  - Open access to specs and discussions
  - Free participation
  - Running code concept
  - No strict timelines
  - Higher document version != fewer changes to expect
  - No official interops (groups organize themselves)

Participating in TLS Standardization

- Important to learn about potential implications and problems ahead of time.
  - Performance implications of certain design decisions
  - Difficulty of integrating new developments into existing code
- Ability to influence the decision making process (particularly since IoT is not the main use case)

- Started implementation work of TLS 1.3 using existing mbed TLS code

A few years forward…

- Specs keep changing (now at version -20)
- More optimizations & more security reviews
- Implementers updated their specs and regularly met at interop events (actually at the IETF Hackathons)

Code: what looked like a small coding project turned into a re-write of our stack.

What was accomplished?

- TLS 1.3 is a re-design of the popular TLS protocol.
  - Makes the handshake faster (Zero-RTT)
  - Shortened algorithm list
  - Improved privacy protection
  - Harmonized extensions

- More formal analysis
- More external involvement

- Specification now in review by the steering group

Lessons learned

- Getting researchers to pay attention to standardization is really hard.
- It worked with TLS 1.3
- Security reviews/formal method analysis did, however, took a long time.

- Writing code during specification phase provides valuable input but is also frustrating.

ARM

Can you help?

- Can we use formal methods in protocol development more aggressively?
- How can we do it in a timely manner?
- Is this the job of researchers or standardization experts?
- What are the best techniques?
- Can we produce code from these formal models/descriptions?
- How can we improve testing (in the style of test-driven development)?

ARM

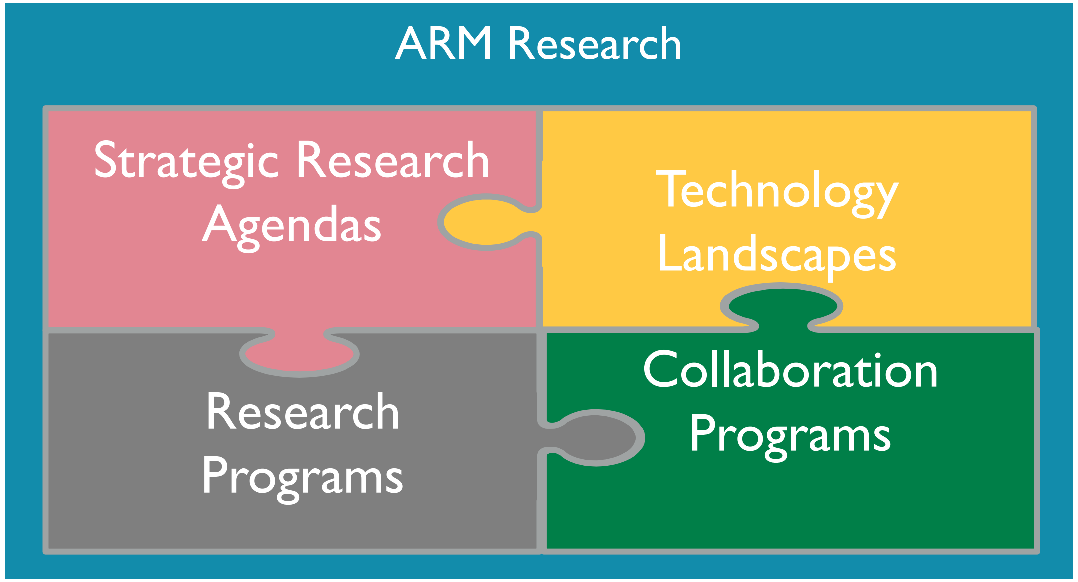
What's next?

- DTLS 1.3 – more optimized version for IoT
- QUIC – a new transport protocol

- We hope to release our mbed TLS 1.3 code to the public soon and do some performance analysis / comparison with earlier versions.

ARM

Introducing ARM Research



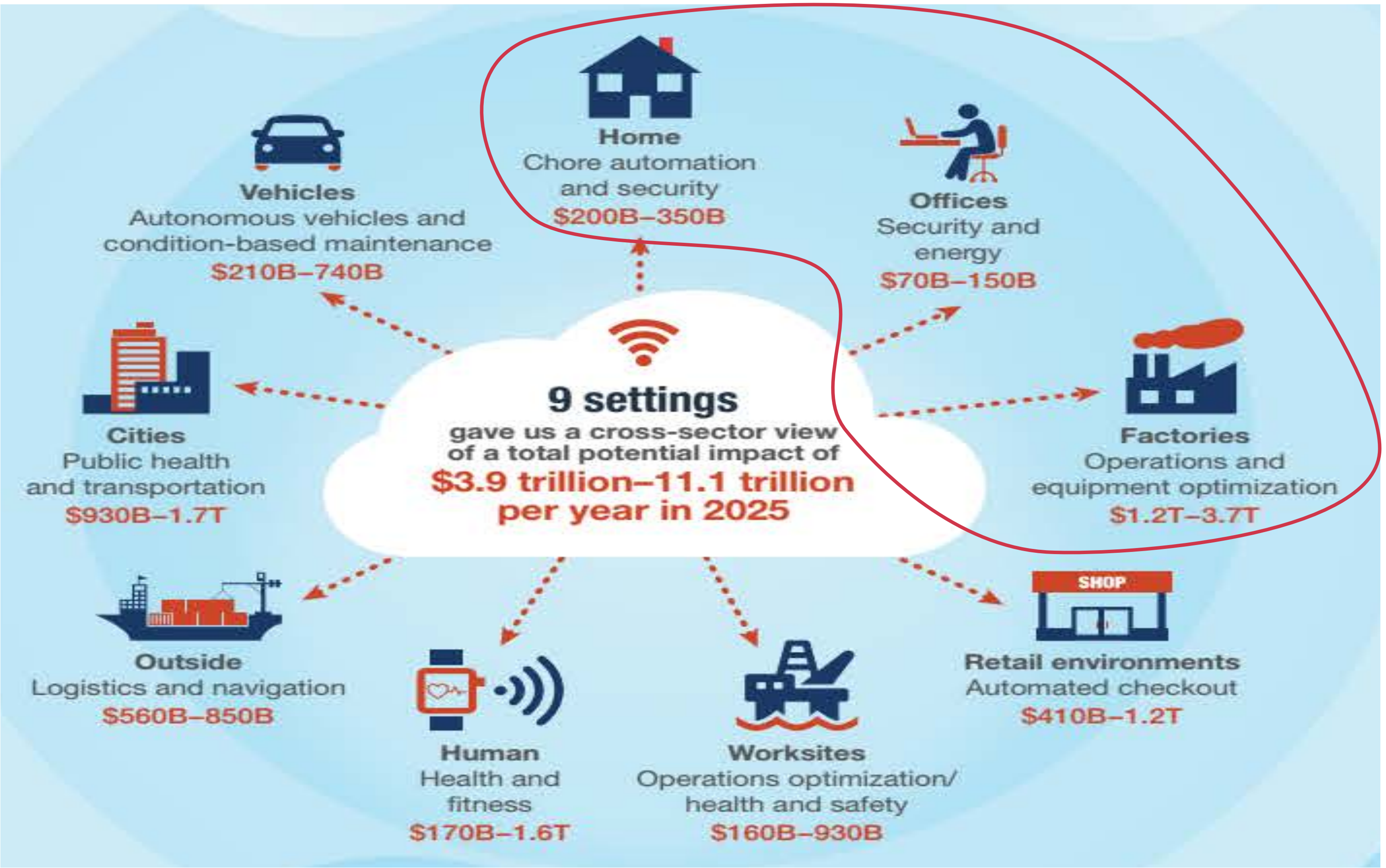
Mission

Partner to accelerate innovation and transfer research knowledge across ARM *and* its ecosystem impacting product success across all markets

Objectives

- Build a pipeline to create and bring future technology into ARM or ARM Ecosystem products
- Create and maintain the emerging technology landscape
- Deliver a consistent stream of architecture innovation in Silicon, Hardware, Software & Services
- Enable innovative Academic research using ARM technologies
- Continuously improve ARM's research capability through regional collaboration and partnership

Highest potential IoT Opportunities ($1-4T) Smart Buildings



Source: Unlocking the potential of the Internet of Things, June 2015, McKinsey

Why Smart ~~Buildings~~ Systems Become Smart

Preventative Maintenance

Monitor equipment, flag performance drifts
Predict/prevent issues, create work orders

Benefits

- Reduce maintenance costs
- Improve equipment performance
- Prevent downtime
- Improve worker and task allocation
- Increase revenue through new business models

Resource Efficiency

Reduce consumption of water, energy, and materials

Benefits

- Sustainability
- Reduce Opex (utility & procurement costs)
- Increase Net Operating Income
- Improve Asset Value

Occupant Comfort
(+ Health, Wellbeing, Productivity, Safety, Security)

Benefits

To Tenants:
- Improve health, wellbeing, productivity and safety of high value and highly expensive occupants
- Reduce absenteeism, vacancy, tenant turnover

To Owners:
- Improve security of occupants, equipment, IP and supply of energy, water and data
- Owners get higher value tenants

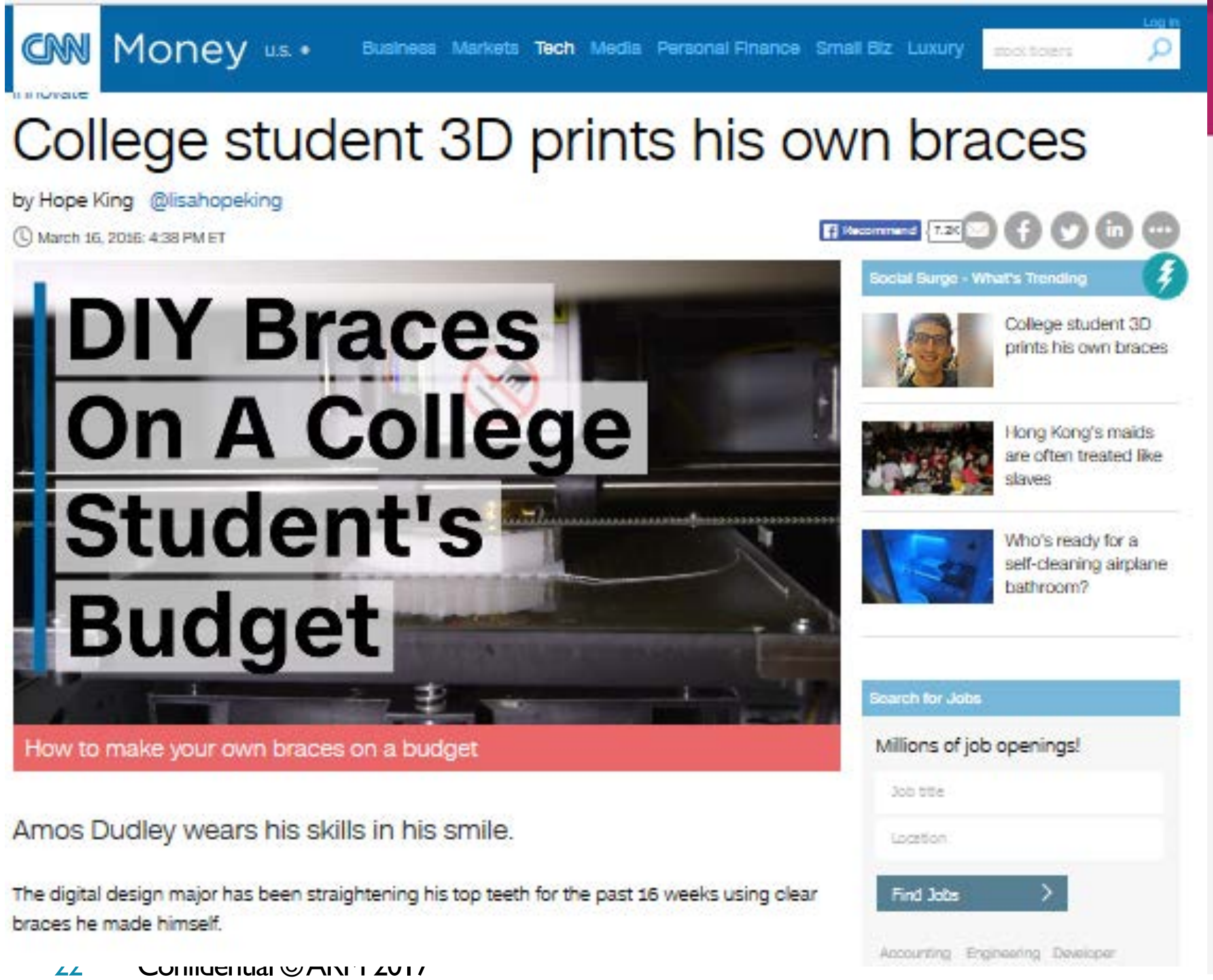
ARM

Trusted Data is critical to telemedicine

Medical data will be priced accordingly to quality, reliability, and provenance.

ARM

Medical device innovations also coming bottom up


CNN Money U.S. • Business Markets Tech Media Personal Finance Small Biz Luxury

Log in

innovate

College student 3D prints his own braces

by Hope King @lisahopeking

March 16, 2016: 4:38 PM ET

How to make your own braces on a budget

Amos Dudley wears his skills in his smile.

The digital design major has been straightening his top teeth for the past 16 weeks using clear braces he made himself.

Social Surge - What's Trending

College student 3D prints his own braces

Hong Kong's maids are often treated like slaves

Who's ready for a self-cleaning airplane bathroom?

Search for Jobs

Millions of job openings!

Job title

Location

Find Jobs

Accounting Engineering Developer


theguardian

US world opinion sports soccer tech arts lifestyle fashion business travel environment science

home › lifestyle › health & fitness love & sex family women home & garden food

Health & wellbeing

Health hackers: the patients taking medical innovation into their own hands

Tired of waiting for a monitor for his diabetes, Tim Omer made his own. He is one of a growing number of patients circumventing medical companies in favour of a homemade healthcare revolution

Ara Darzi

Monday 26 October 2015 03.20 EDT

Shares 894 Comments 101

Save for later

Tim Omer and part of the monitoring kit he built himself - the receiver re-using a Tic Tac box. Photograph: Linda Nylind for the Guardian

Tim Omer is a 31-year-old diabetic. Rolling up his sleeve, he reveals a small box, about half the size of a cigarette packet, taped to his upper arm. From the box, a sensor runs under his skin, delivering a readout of his blood glucose level to his mobile phone.

This is something to which few Type 1 diabetics in Britain have access - the monitors cost around £4,000 a year to buy and maintain and are too expensive for the NHS.

ARM

GE Lighting

LightGrid™

Smart Cities

Deployed in **over 20 cities** in the US and in Latin America including:

- San Diego
- Oceanside
- Chicago
- Atlanta
- New York

90 Smart cities by 2025

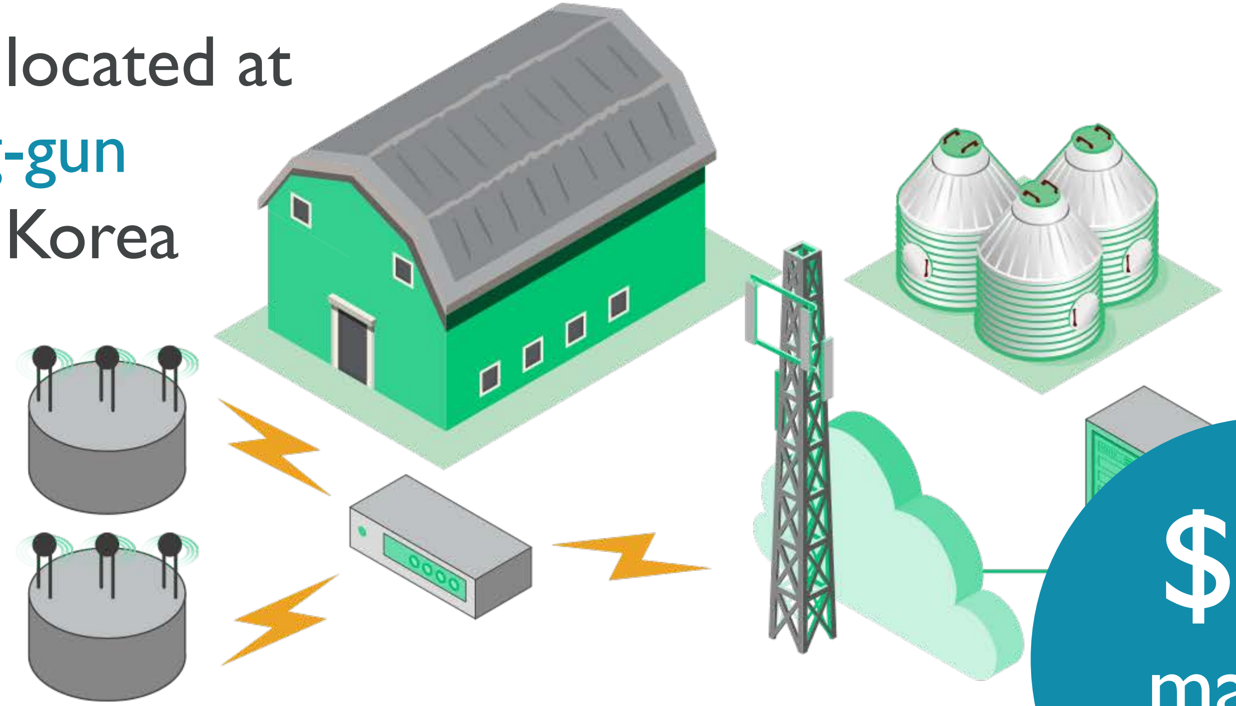
5.3B connected devices by 2020

+$4.5B in next 5 years

ARM

SK telecom – Fish farming

Test site located at
Gochang-gun
in South Korea



Precision farming

10B
people
In 2050

$5B
market
in 2020

+70%
food
production

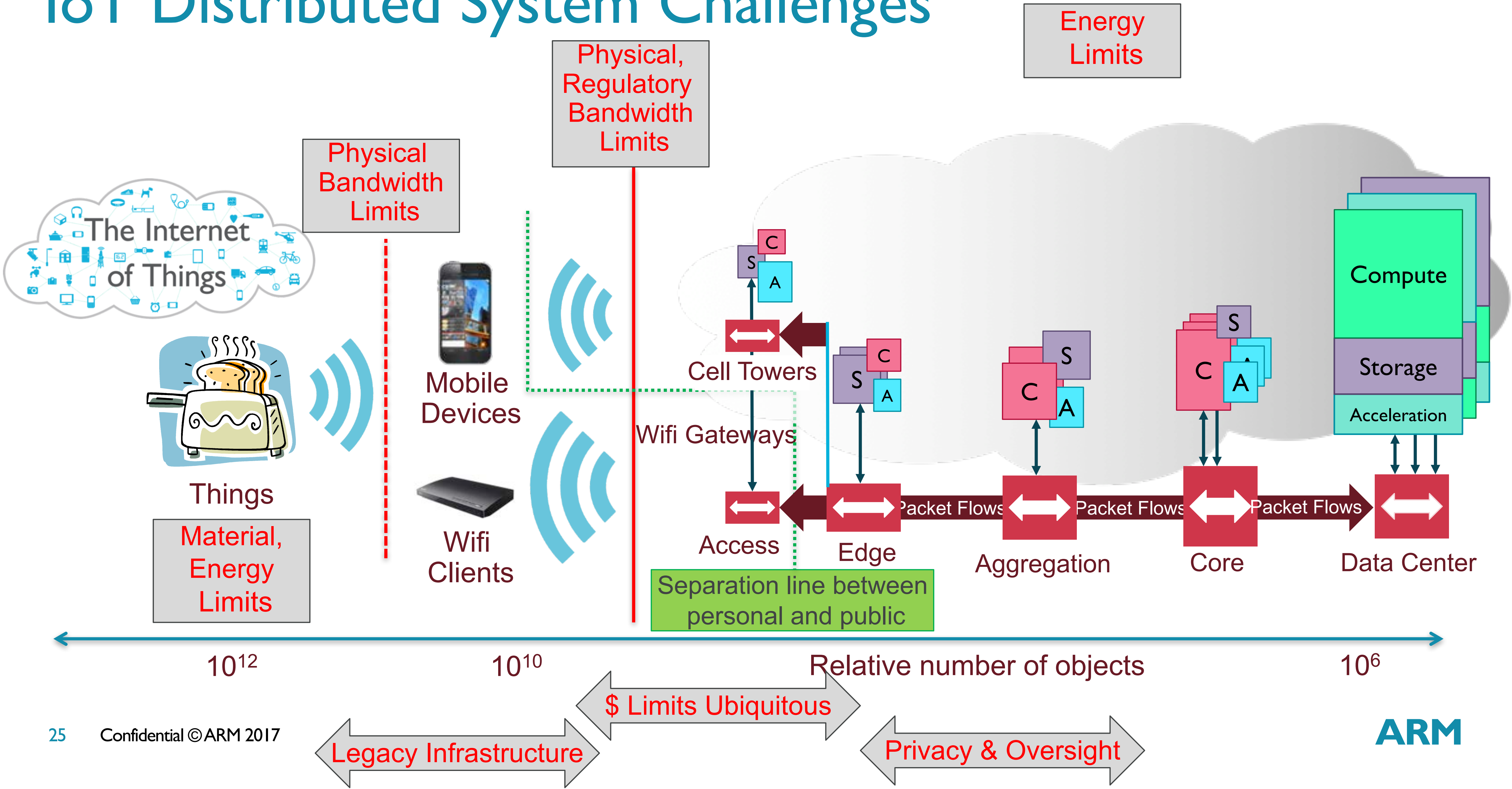
Sensors	IoT Router	Network	Io…	…w E…
Temperature pH, DO		LTE / 3G		

mbed mesh, mbed OS

mbed Device Server

ARM

IoT Distributed System Challenges



ARM

Data Lifecycles

- (New) 'IoT Applications' generate and use huge data sets
- Local 'in application' walled garden
- Import and Export (from Marketplace) for Data Fusion
- Live Inference
- Long term Learning Models

- Privacy & Consent Preserving Information Models and Manifests
- Full Data Lifecycle Identity & Attestation
  - Management and removal of consent
  - Change of ownership
  - Change in Policy
- Automation for Smart Contracts

ARM

Some ISG Research Agenda Key themes

- Distributed System = End to End - Edge to Cloud
  = Top to Bottom - Hardware Firmware Application
- IoT Application – apply to any value adding Smart (City building Transport Factory Helathcare etc etc)

- Distributed IoT Systems Architecture & Optimization
  - Delegated Applications computing
  - Delegated Secure Systems Management (assume always compromised)
  - Delegated Secure System Lifecycle Management
- Data Brokering Systems Architectures
  - Live and Archived
- Distributed Systems Vulnerability Analysis

- Distributed Systems Modelling & Tuning (digital twin)
- Distributed Systems Programming and Development
- HCI and Design factors for Secure System Usage and Operation

- Privacy/Consent Preserving Information Manifests
- Warranty, Ethics & Policy influences on system constraints

ARM

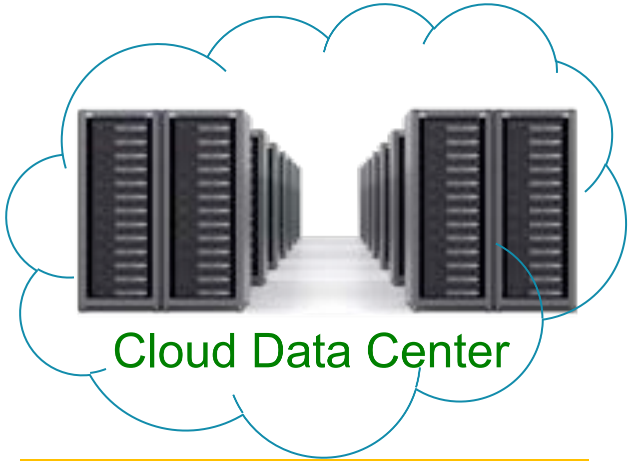
Systems Architecture: Distribution & Delegation & Lifecycle

Clients

- Device & Communication Duty Cycles
- Application Processing 'Fog'
- Latency Sensitive Tasks
- Learning and Inference
- Delegated Security
- Adaptive Networks

- Lifecycle Challenges and Costs a first order issue

- Network Systems Service Operation
- Privacy & Security Service Operation
- Secure Software Update
- Fleet Asset Management and Field Maintenance



Cloud Data Center

STANDARDS BASED PROTOCOLS MANDATED

Mix of NFV, SDN, IT-Management Technologies
(e.g. deployment tools)

Access Points @ network edge

Broad Distribution Of Optimized Heterogeneous Compute Solutions

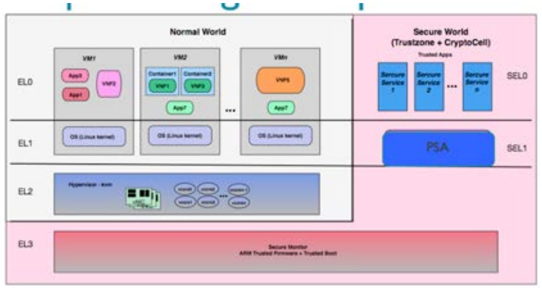
Security

ARM Research Driven by Device Co-Design

Key Application Classes

- **AI/ML**
- **HPC**
- **HPDA**

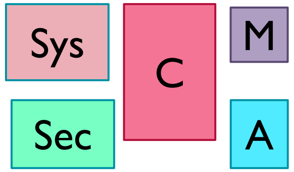
Application Payload | Secure Communication | Secure System Management

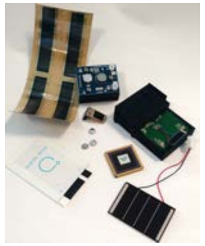


Device ARCHITECTURE

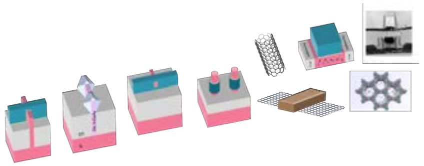
- **VM/Container**
- **TEE/REE Isolation**
- **Hypervisor**
- **Monitor**

- **Compute**
- **Memory**
- **Acceleration**
- **System**
- **Security**





Energy Harvesting

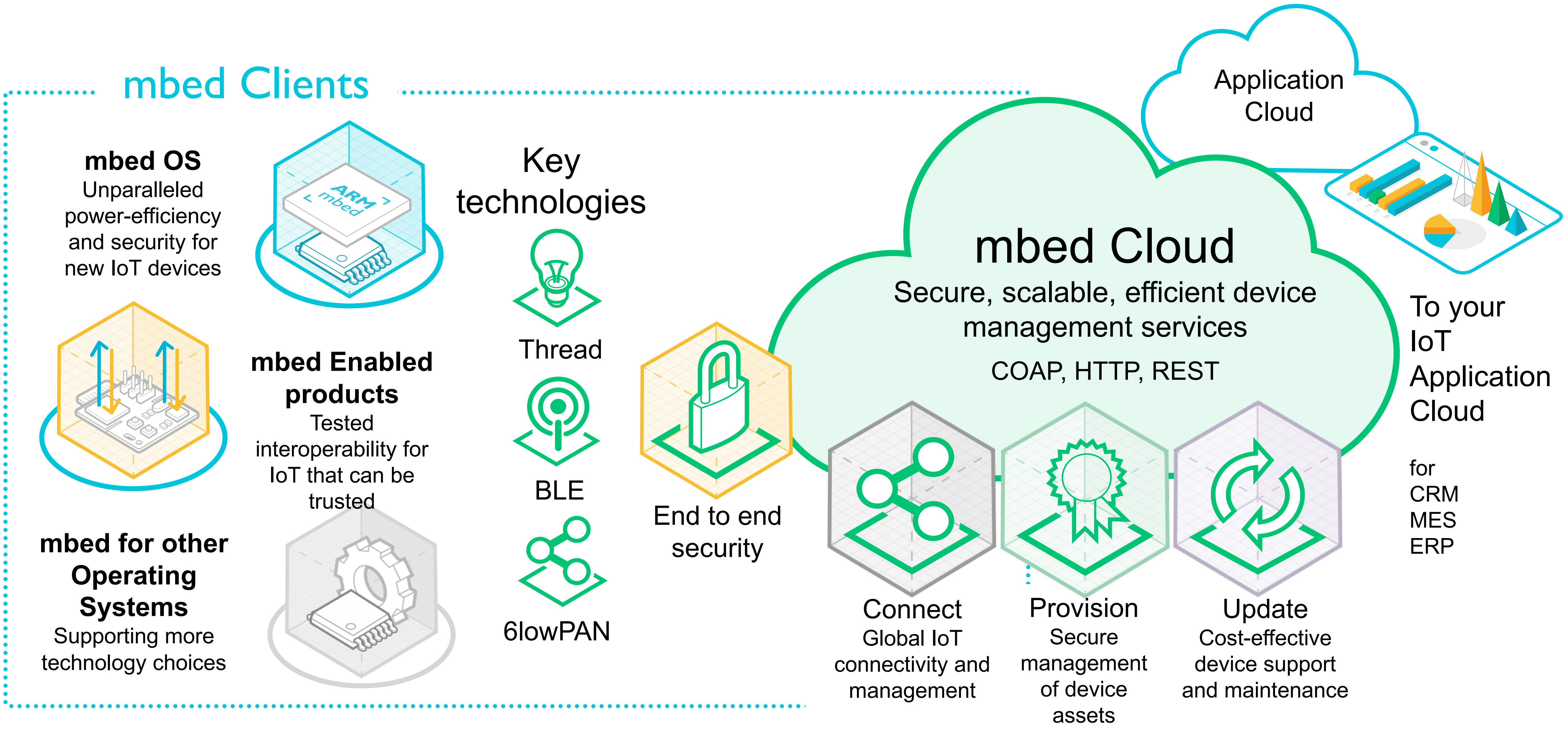


Future Silicon

- Every Node in the Distributed System operates within a Constrained Environment
- The local Application Communication and Management Payloads must be optimized
  - Energy
  - Throughput
  - Latency
  - Physical Size
  - Threat Model
  - Cost
- Product portfolio and ARM Licensing mode enables optimal response

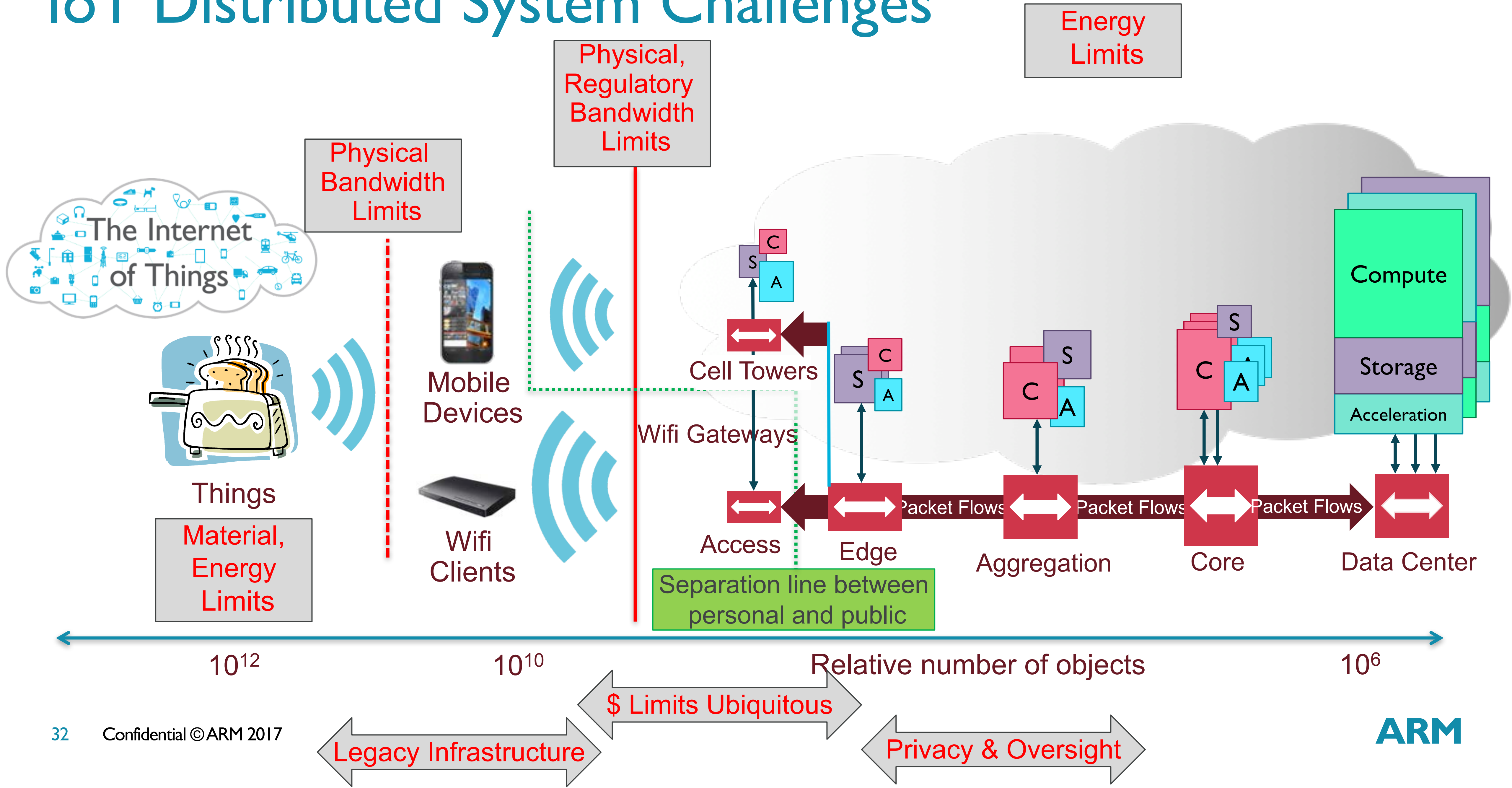
ARM

mbed IoT device platform: device services for scale



ARM

IoT Distributed System Challenges



ARM

Security is Top to Bottom and End to End

- COMPOSABLE SYSTEMS
- REFINED ARCHITECTURE
- ALWAYS COMPROMISED