ARM Perspective on the Internet of Things

Midi Minatec, October 24th 2014
Remy Pottier Director of Strategy ARM
The IoT Opportunity is much larger
Analysts predictions for connected devices (2020):

- 30 billion?
- 50 billion?
- 75 billion?

The IoT Market is growing
Not a new concept, it’s been around for >20 years\(^1\)
Connected things > world population (6.8B)

---

\(^1\) Weiser, Mark (1991) “the Computer for the 21st Century”
The term Internet of Things was proposed by Kevin Ashton in 1999
Over 3 Billion

ARM® Cortex® -M devices shipped in 2013 by leading semiconductor companies

MCUs
radios
sensors

Canalys
Deloitte
Idate
ABI Research
Strategic Analytics
Cisco
Idate

2025
2.7T
McKinsey
2016
36B
Idate
2014
17m
Canalys
2014
10m
Deloitte
2013
10B
Cisco
2020
68B
2020
50B
2018
92m

Watches
Bands
Glasses
Wearables

0.5m
92m
125m
32m
125m
10m
20m
2.7T
68B
2017
20m
Strategy Analytics
2017
125m
Strategic Analytics
2020
50B
55m
2020
20m
Strategy Analytics
2017
125m
Strategy Analytics
2020
68B
68B

10 billion chips in 2013

Courtesy of Vianney Courbon – Orange
IoT Segments

- IoT is not a single market
- Multiple ecosystems
- Thus variety of performance, cost and security requirements
  - Personal devices are cost sensitive and largely focused on monitoring
  - Commercial devices require more robust security for data handling and control system management
What are the key components of IoT?
Connected appliances
Remote control
City-scale analytics
Quantified self
Analytics
Web services
Outpatient care
Monitoring
Data quality
Quick response
Tracking
Aggregation
End use
Smart Buildings

Device + User + Data (little/big) + Cloud + Analytics + Apps + Web services

how they are connected? common horizontal technology to connect the dots?
Is there anything New about IOT or has it Just Become Fashionable?

Where is the value?
Building Management

What's new?
• It Learns?
• Gives user control?
• (new) services?
• Data value for something else?
• Helps you save energy?
• It's fashionable
• a consumer application with easy to use interface?
Connectivity bring the processing power of supercomputer, and analytics from the cloud, to small devices.
Change the relationship between user, devices and services

Functional Becomes IOT Little Data / Leveraging “Big Data” enables services revolution
Problems to solve
Current IoT market limitations

- Fragmented industry verticals:
  - The IoT “wheel” is reinvented from industry to industry

- Customized solutions abound:
  - Each solution has its own design, production, and implementation cycle, customized hardware
  - Software design is limited to a small group of developers who understand the architecture and API’s for a particular industry or platform, thus leading to high development and support cost

- Lack of scale for components:
  - Economies of scale are difficult to achieve in any given industry since solutions are so varied and unique.

- Need to break “silos”
Zoom on Problems to solve for OEM – similar across verticals

Develop the *Things* and then …

- **Differentiate and innovate**: Connected capabilities enable end users and customers to reinvent their user experience thanks to the connected products.

- **Integration**: Need to work with enterprise or other consumer systems and software.

- **Security**: Enable this to be done securely by authorized machine or people - Users and Things authentication – to protect privacy and data integrity.

- **Enable Services development/deployment**: Serviceable: Enable easy and quick applications and services development and deployment.

- **Enable Data/devices Management**: Enable big data management - provisioning, reporting, storage, to create knowledge and intelligence through simple UI.

- **Enable Connection**: Connected: Enable to find and connect any *Things* to the internet easily and automatically.
Market Development Problem to Solve

Internet of Things

- Scale needs interoperability
- Interoperability needs Standards
- Sharing needs Trust
- Trust needs Security

Today

Silos of Things
Everything nearly connects

Reach

Internet Of Things

Open Data and Objects
Smart Everything
Sensors & Actuators Networks

Applications
Mobile internet
Internet / broadband
M2M
SaaS

Fixed Telephony Networks
Mobile Telephony
Scale Needs Standards
Plenty of IoT / M2M standards to choose from

>120 standards relevant to IoT

- **Horizontal**
  - 3GPP, 3GPP2, ACM, AHCJET, AIM, AllSeen Alliance, ANCE, Bluetooth SIG, CINTEL, CITEL, Hart Communication Foundation, IETF, IPSO Alliance, MIG, MQTT.org, NFC Forum, ngConnect, NYCE, OASIS, ODVA, OGC, ONVIF, Open Interconnect Consortium, OSGi, PUCC, SD Card, SIM Alliance, TCG, Thread, W3C, WAVE2M, ZigBee Alliance

- **Automotive**

- **Healthcare**

- **Home Automation**
  - ASIS Int’l, Aureside, BACnet, Broadband Forum, CABA, EnOcean Alliance, HGI, Home Grid Forum, Home Plug Alliance, KNX, OBIX, PSIA, SIA (security), Z-Wave Alliance

- **Industrial**
  - AIA, Automation Federation, CiA, Industrial Internet Consortium, ISA, M-Bus, Modbus, OACARI Alliance, OMAC, OPC, SMLC

- **Utilities, Smart Grid**
  - AAPA, CIGRE, DLMS, DRSG Coalition, EDSO, EEE, ENTSOE, ESMKIEG, Eurelectric, EUTC, Gridwise Alliance, Gridwise Architecture Council, JSCA, NEMA, NIST, T&D Europe, TIA TR-51, UCA, UTC Smart Network Council, UTC

- **Supply Chain**
  - AIM, APICS, CSCMP, GS1, ISM, SCM, XBRL Int’l

- **ITU GSC (Global Standards Collaboration) members**
  - ITU-T, ARIB, ATIS, CCSA, ETSI, ISACC, TIA, TTA, TTC

- **ITU GSC observers**
  - 4G America, AICTO, CDG, GISFI, GSMA, IEC, IEEE, ISO / IEC JCT, OMA, SCTE
Navigating IoT Standards – simplified view

Many app frameworks
- Vertical, horizontal
- Open, proprietary

Examples:
- IPsec
- OTA
- OMA
- UpnP
- LLSEEN
- ALLIANCE
- OPEN INTERCONNECT
- CONSORTIUM
- Continua

Application Level
- REST
  - EXI | XML | JSON payload
- RPC / RMI
- CoAP
- HTTP
- DTLS
- TLS
- UDP
- UDP | TCP
- 6LoWPAN
- IPv4 | IPv6
- 802.15.4 MAC / PHY

Internet Level
- 802.11 MAC/PHY
- 3GPP | LTE
- BT MAC/PHY
- IEEE 802.15.4 MAC / PHY

Network Level
- Bluetooth
- ZigBee
- ZigBee Cluster Lib
- ZigBee App Layer
- ZigBee Network Layer
- Security Manager
- Host Control I/F
- L2CAP | IP | UDP

Networking protocols
- 6LoWPAN
- IPv4
- IPv6
- UDP
- TCP
- CoAP
- HTTP
- TLS
- DTLS
- HTTP
- HTTPS
- SSL
- TLS

Internet + Web to the edge...

for constrained networks, devices

For constrained networks, devices:
- Many app frameworks
- Vertical, horizontal
- Open, proprietary

Examples:
- IPsec
- OTA
- OMA
- UpnP
- LLSEEN
- ALLIANCE
- OPEN INTERCONNECT
- CONSORTIUM
- Continua

Higher performance devices / networks

Constrained devices / networks
From Web Applications to IoT Nodes

Application
1000s of bytes

Web Object

HTTP

TLS (TCP)

IPv6

IPv6 → 6LoWPAN
  • Header compression on sensor networks

TCP → UDP
  • No guarantee of packet delivery or order

HTTP → CoAP
  • HTTP-like (REST) semantics for constrained devices

TLS → DTLS
  • TLS over UDP – stateless – one packet at a time

IOT Backhaul
100s of bytes

Binary Web Object
CoAP
DTLS (UDP)
IPv6

IOT Sensor Network
10s of bytes

Binary Web Object
CoAP
DTLS (UDP)
6LoWPAN

Proxy

Gateway
Sharing Needs Trust
Who can get access to my data?

- **Machine Utilization**
- **Equipment Owner**
- **Service Contract**
- **Personal Planner**
- **Personal @ Gym**
- **Personal @ Facebook**
- **Personal Reward**
- **Health Provider**
- **Hospital**

### Gym
- Machine ID
- Personal ID
- Start Time
- Stop Time
- Distance
- Exercise Profile
- Heart Rate

### Weight
- Device ID
- Personal ID
- Date / Time
- Scale (Kg/Lbs)

### Cycling
- Bicycle ID
- Personal ID
- Start Time
- Stop Time
- GPS Mapping

### Running
- Personal ID
- Start Time
- Stop Time
- GPS Mapping
- Heart Rate
Trust Needs Security
IoT Security

- Can a pacemaker be hacked to kill?
- Or just a plot line in US TV series

- Security is critical to all IoT devices

- Initial IoT devices already being broken
  - Hue LED lights – remote control
  - Fridge sending out spam / DDoS

- Massive issue for industrial systems
  - Stuxnet & Flame well known threats
  - Biggest threat to Critical National Infrastructure

This should not be an afterthought!
Device security: How much is enough?

All connected devices require some level of security.

Complexity

- Life Enhancing
- Fitness
- Home Automation
- Personal Healthcare
- Mainstream Healthcare, Smart Cities, National Critical Infrastructure

Integrity & Privacy

Cost Sensitive Applications

Real Life Impact

Mainstream Applications

Public Safety

High Security Applications

Impact of Attack

- Loss of privacy is bad.
- Attack on critical infrastructure may be catastrophic

All connected devices require some level of security.
ARM in IoT
Enabling Efficient Sensor Nodes

Over 2 Billion
ARM® Cortex® -M devices shipped in 2012 by leading semiconductor companies

MCUs  radios  sensors

ARM® Cortex®-M0+
Freescale Kinetis KL03
1.6 x 2.0 mm
Little Data Enables Big Data

ARM® mbed™
IoT Device Platform

mbed OS

IP and Web to the edge

mbed Device Server

IoT Service or App

End-to-End Security, Web, Data Objects & Management

Little Data

BIG DATA
Summary

- IoT silicon opportunity – 30..75B devices by 2020
  - Mostly small devices woven into the fabric of our physical and digital lives

- Internet/Web protocols can scale to meet the needs of IoT

- Security is essential – and the standards are already in place
  - Every device needs a secure key store and basic crypto support

- Create trust between devices, applications and users

- The result: Trustworthy IoT at Internet/Web scale!
Thank You

The trademarks featured in this presentation are registered and/or unregistered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Any other marks featured may be trademarks of their respective owners.