Internet of Things
Decoding the IoT Ecosystem
Who’s joining the game

Samsung snaps up SmartThings, embracing Internet of Things
The tech giant acquires the open platform for smart home devices to “improve the convenience and services in people’s lives.”

Huawei buys Cambridge Internet of Things pioneer Neul

Ericsson buys MetraTech to muscle in on IoT

SAP Announces €2 Billion Investment Plan, New Innovations, Acquisitions and Network of SAP IoT Labs to Unlock Next Wave of Value from the Internet of Things

Oracle broadens IoT cloud offering with four new solutions
The outlook for 2020

- Predictions for number of connected devices
  - Gartner: 20.4 Billions
  - IHS: 30.7 Billions
  - Cisco: 50 Billions
  - Intel: 200 Billions

During 2008, the number of things connected to the Internet exceeded the number of people on earth.
Value Creation

- Revenue
- Citizen Experience
- Jobs
- Productivity
- Cost Control

- 4500 New Companies
- 56000+ New Jobs
- 10.5B $ Revenues / year

Jad El Cham | RIPE75 | October 2017
Overview

• The business background
• The IoT Ecosystem
• From sensor to data challenge
• The IoT Data Flow
• IoT Access Technologies
• IoT Security Challenges

Will not cover:

• Smart Device’s IoT
Use cases and Opportunities

- Smart water/gas metering
- Public lighting
- Smart building
- Smart parking
- Assets Tracking
- Smart Agriculture, i.e. leak detection and irrigation
- Water level and flood management
- Fault management
- Security services, i.e. Smoke detectors
- Smart energy and fast demand response
- Waste management
- Traffic management

Source: Cisco
The IoT challenge
The IoT Data Flow

Site

Things → Nodes and Gateways
The IoT Data Flow

Site

- Things
- Nodes and Gateways

Network

- Connectivity
- Backbone (IP?)

Diagram illustrating the IoT data flow from site to network, showing various components and connectivity methods.
The IoT Data Flow

Site
- Things
- Nodes and Gateways
- Connectivity

Network
- Backbone (IP?)
- Data Ingestion

Cloud / DC
- Data Analysis
- Processes and People

IoT Enabler

DATA STREAMS  BIG DATA PLATFORM
The IoT Data Flow - Site

- Part of Operational Technology
- Things can be sensors with analog or digital outputs
- Sensors are powered by the IoT nodes or power sources
- Encoding can be done using MQTT, CoAP, etc.
- Many sensors (Things) can be connected to an IoT node
- Many IoT nodes can be connected to an IoT Gateway
The IoT Data Flow - Network

- Challenge of transporting the data on a massive scale
- Impact on the battery / power source of the source device
- Low Power Wide Area (LPWA) as an IoT Enabler
- Possible Deployment scenarios today:
  - Sigfox
  - LoRaWAN
  - NB-IoT, LTE-M, 5G(?)
  - WiFi + 3/4G
  - Zigbee + 3/4G
**IoT Access Technologies Landscape**

- **Long Range**
  - 2G
  - 3G
  - 4G
  - 5G
  - Wi-Fi .b, .g, .n
  - Wi-Fi .p
  - Wi-Fi .a
  - Wi-Fi .ac
  - Wi-Fi .ah
  - 802.15.4
  - 802.15.4 g/e
  - W-HART
  - ISA 100.11a
  - 6Tisch
  - ZigBee
- **Medium Range**
  - 802.15.4
  - 802.15.4 g/e
  - W-HART
  - ISA 100.11a
- **Short Range**
  - B-LE

**Use Cases support**
- Utilities
- Industrial
- Smart Cities
- Agriculture
- Transportations
- Assets management

- Power consumption very sensitive to endpoint
- Low data rate applications
- Open technology – Ecosystem for solution

**Source:** Cisco / Actility
The IoT Data Flow - Network

Network

Technology Decision Factor
IoT Access Scenarios
## What is 5G?

<table>
<thead>
<tr>
<th>Uses Cases &amp; Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
</tr>
<tr>
<td>Voice + SMS</td>
</tr>
<tr>
<td>200 KHz Channels Below 2 GHz</td>
</tr>
<tr>
<td>Spectrum</td>
</tr>
<tr>
<td>Radio Technology</td>
</tr>
<tr>
<td>GSM/GPRS (Single Technology)</td>
</tr>
<tr>
<td>Network Technology</td>
</tr>
<tr>
<td>Macro Cells</td>
</tr>
<tr>
<td>Source: InterDigital</td>
</tr>
</tbody>
</table>
What 5G is

• The hyper-connected vision
  ○ Blend of pre-existing technologies (2/3/4G, WiFi, etc.) for higher coverage and availability
  ○ Key differentiator being greater connectivity as an enabler for M2M and IoT
  ○ May include a new radio technology to enable low power, low throughput field devices

• Next-generation radio access technology
  ○ More of a traditional ‘generation-defining’ view
  ○ Specific targets for data rates and latency being identified
  ○ Easier determination of whether a technology is 5G or not

• The two views described are regularly taken as a single set and hence views are grouped together
What 5G is

Simultaneous connectivity across 5G, 4G and Wi-Fi

Source: Qualcomm
Technology Requirements for 5G

- 99.999% Availability
- 100% Coverage
- 90% reduction in Network energy

- >10 Gbps peak data rates
- 100 Mbps whenever needed
- 10-100 x more devices
- 10 000 x more traffic
- M2M ultra low cost
- <1 ms radio latency
- 10 years on battery
- Ultra reliability
- 99.999% Availability
- 100% Coverage

For everything

Instant action

Unlimited experience

Extreme Mobile Broadband

Massive machine communication

Critical machine communication
Use cases for 5G

- Extreme throughput: Multi-gigabits per second
- Ultra-low latency: 1ms E2E latency
- Uniform experience: much more capacity
Use cases for 5G

- **Power Efficient**: Multi-year battery life
- **Low complexity**: Low device and network cost
- **Long range**: Deep coverage
Use cases for 5G

- High reliability
  - Extremely low loss rate

- Ultra-low latency
  - 1ms E2E latency

- High availability
  - Multiple links for redundancy and mobility
Implications of 5G on Operators

- Operators need to overcome a series of challenges if the 5G benefits are to be realised
- 5G spectrum and coverage implications

Below 1 GHz: longer range for massive IoT

1 GHz to 6 GHz: wider bandwidths for enhanced mobile broadband and mission control

Above 6 GHz (mmWave): extreme bandwidths, shorter range for extreme mobile broadband

From wide area macro to local hotspot deployments
Support for diverse network topologies (D2D, Mesh, etc.)
Implications of 5G on Operators

• Operators need to overcome a series of challenges if the 5G benefits are to be realised

• < 1 ms Latency
Roadmap for 5G

By the second half of 2017 the focus of our work will shift to Release 15, to deliver the first set of 5G standards - including new work as well as the maturing of the LTE-Advanced Pro specifications.

www.3gpp.org
The IoT Data Flow - Cloud / DC

- Big Data applications for IoT
- Many solutions by Cloud Software Providers
- Interface for humans to understand the data and interact with it
- Automated processes based on the input received
- Machine Learning, AI, M2M
IoT Applications Models

- **IoT Data Services and Apps**
  - Manufacturing / Utility / Oil & Gas / Transportation / Healthcare / Cities / Retail

- **IoT Data Platform (IoT Cloud)**

- **IoT Fabric**
  - Devices / Sensors / Actuators / Silicon / Device Security
IoT Services Framework

Data Management

Device Management

Connectivity Management

SECURITY

Applications
Integration with other Systems
Data streaming between clouds

IoT Services Framework

IoT Services Framework
Fog Computing

- Computing done on the IoT Gateway
- Linux OS gateways and nodes, local computing possible
- Reduce the chatter on the transmission medium
- Push some intelligence towards the edge
Mist Computing

- Some decisions taken at the source
- Discard useless information
- Data processed faster at destination
- Processing done on the level of the sensors
IOT Security
101
IoT Security Landscape

• No one definition of IoT
  ○ Internet connected device
  ○ Characterised by a constantly growing network of connected devices and actuators that can sense or interact with their internal states or the external environment (Europol - iOCTA)
  ○ Smart Devices
  ○ Consumer Devices / Industrial Control Systems
  ○ Emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context (ENISA)
IoT Security Challenges

- Many more devices on the network
- Lack of security updates and patches for remediation by vendors
- Weak or no encryption / Data Protection
- Devices running old services with vulnerabilities
- Lack of computing power on many IoT devices
- Security by design not a concern to some vendors
- Lazy consumers
- Undocumented hard coded passwords
IoT Security Impact

- Devices become part of an IoT botnet
- Devices are bricked or destroyed
- Health related impact (connected medical devices)
- Compromised privacy
- Data theft
- Full networks compromise
- APTs
Access to IoT Devices

- If an IoT Device is not accessing the internet, it does not mean that it is not accessible from the Internet!!!
- Port Forwarding
- UPnP: Universal Plug and Play, widely used today, when you buy a device, it tells your router to expose the device from the internet dynamically
- 275 000 IP cameras exposed to the internet today without users knowing it because of UPnP
IoT Victims

- Victims can be:
  - Unauthenticated devices
  - Devices with default credentials
  - Devices with strong password but with weak security embedded components
  - Devices with a backdoor account that grants privileged access
  - Devices with old firmware
  - Devices that do not contain fixes to security vulnerabilities
  - ANY DEVICE
DEMO
Access to IoT Devices
Vulnerability Research Statistics - ICS

Source: Kaspersky LAB ICS CERT - H1 2017
Vulnerability Research Statistics - ICS

Source: Kaspersky LAB ICS CERT - H1 2017
Vulnerability Research Statistics - ICS

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>31</td>
</tr>
<tr>
<td>Engineering</td>
<td>24.5</td>
</tr>
<tr>
<td>Education</td>
<td>14.5</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td>9.7</td>
</tr>
<tr>
<td>Energy</td>
<td>4.9</td>
</tr>
</tbody>
</table>

Source: Kaspersky LAB ICS CERT - H1 2017
Vulnerability Research Statistics - ICS

Source of Vulnerability - Europe

Source: Kaspersky LAB ICS CERT - H1 2017
### Vulnerability Research Statistics - ICS

**Percentage of ICS computers affected**

- **Internet**: 20.4%
- **Removable Media**: 9.6%
- **Email Clients**: 3.9%
- **Windows Backup**: 0.3%
- **Archives Backup**: 0.3%

**Source of Vulnerability - World**

*Source: Kaspersky LAB ICS CERT - H1 2017*
How do we protect ourselves?

- Expose devices to the internet only if you need it; use VPN when possible
- Place IoT Devices on a separate VLAN
- Always change default credentials
- Turn off UPnP
- Always update devices to latest firmwares with latest security patches
- Select carefully your cloud services
- Give preference to known vendors
- Digital hygiene across the network, not only IoT devices
IoT security efforts and initiatives

- **Community effort** - *i.e. AIOTI, Project OWASP for the IoT*


- **Governmental Regulation** - *Internet of Things Cybersecurity Improvement Act of 2017*

- **Governmental Guidelines** - *US DHS Strategic Principles for securing IoT*

- **IoT Security Guidelines** - *GSMA IoT Security Guidelines & Assessment*

- **Public Awareness** - *IoT Security focused workshops and conferences*
Smart Cities

Today
Nice - Connected Boulevard

- Congestion reduced by 30%
- Air pollution and noise levels reduced by 25%
- Savings between 20 and 80 % in areas such as street lighting and light management
- Parking income increased by 30%
- Better citizen experience

Image credit: Flickr
Dubai - Smart City

- 40% of city centre traffic caused by parking issues
- Driverless transport set to be common in 2020
- 1000 government services smart by 2017
- Potential investment value of AED 17.9 billion by 2019
- 250 000 Smart meters for Electricity and Water
San Francisco - Connected City

- The goal is to achieve a 10% Shift
- Shift 10% of single-occupied vehicles to public transit
- Reduce 10% in transportation emissions
- Reduce accidents and fatalities by 10%
- Reduce 10% in resident’s spending on transportation
- Repurpose unused traffic lanes for a better CX

Image credit: Curbed IM Photo
Oslo - Sustainable City

• 50% reduction in emissions of greenhouse gases by 2020

• 95% climate neutral city by 2030

• 2/3 reduction in energy consumption for street lighting

• Reduction of health care costs by providing flats with assistive technology and smart interior design

• Open data initiative

Image credit: ScandicHotels.com
Why should the RIPE community care?

• The IoT is by all means a massive phenomenon with disruptive implications
• Affects directly the Internet
• Security concerns in the background
• IoT cannot be approached in a conventional network-based mindset
• The RIPE community is highly interested in the IoT direct applications
• Direct effect on number resources??
Questions

jelcham@ripe.net