Security – Essential for the Growth of M2M and IOT
Mobile World Congress Shanghai – 16th July 2015
Shane Rooney – Executive Director GSMA
About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.
IOT Market Potential for Operators by 2020

2014
12.6 Billion Total Connected Devices

2020
27 Billion Total Connected Devices

2020 Addressable Opportunity for Operators in selected vertical sectors*

- Connected Health: $31 Billion
- Connected Car: $135 Billion
- Connected Industry: $18 Billion
- Connected Living & Working: $188 Billion
- Connected Cities: $26 Billion
- Connected Cities: $26 Billion
- Connected Cities: $26 Billion
- Connected Cities: $26 Billion

Total Addressable Opportunity For Mobile Network Operators in 2020

$1.1 Trillion

2014
7.3 Billion Mobile Connected Devices

2020
10 Billion Mobile Connected Devices

PCs/Handsets/Tablets
$ 687 Billion

North America
$261 Billion

Europe
$271 Billion

Latin America
$76 Billion

Middle East
$64 Billion

Asia Pacific
$413 Billion

CREATING OPPORTUNITIES THROUGH CROSS-INDUSTRY COLLABORATION
GSMA Connected Living Programme
MOBILISING THE INTERNET OF THINGS – ENABLING GROWTH & OPPORTUNITY

MARKET GROWTH

Connected Living Programme
Scaling the Cellular IoT

<table>
<thead>
<tr>
<th>Cellular M2M Connections</th>
<th>Compound Annual Growth Rate (CAGR)</th>
<th>No. of devices (billion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020 Forecast</td>
<td>Dec 14</td>
<td>0.8</td>
</tr>
<tr>
<td>2020 Growth target</td>
<td>Dec 15</td>
<td>0.6</td>
</tr>
<tr>
<td>970m</td>
<td>Dec 16</td>
<td>0.4</td>
</tr>
<tr>
<td>1.25bn</td>
<td>Dec 20</td>
<td>0.2</td>
</tr>
</tbody>
</table>

Source: GSMA Intelligence

MARKET OPPORTUNITY

Total Addressable Market for Mobile Network Operators in 2020
$1.1 TRILLION

Increased operator role and revenue opportunity

Total Addressable Market for Mobile Network Operators in 2020
Source: Machina Research

FOCUSED DELIVERY ON KEY MARKET ENABLERS

Unifying the IoT
Common Global Specifications

Customer Focused Service - Remote SIM Provisioning

Managed Connectivity

ECOSYSTEM ENGAGEMENT

Active Industry Engagement Vertical Markets - Automotive, Transportation, Utilities and Health

Demonstration & Encouragement of IoT Innovation

© GSMA 2015
Operators enable the market throughout the value chain.

Operator value starts with connectivity and increases up the chain.

Simple Valuable Business Model

Lower cost driver premiums

Traditional insurance - £3k
Connected Insurance - £1.4k

UK driver aged 17, annual premium actual data 2014

Insure the Box, the parent company after 4 years valued at £140m, 2014
How to get involved in the Connected Living programme?

**GSMA Connected Living – “Mobilising the Internet of Things”**

- **Remote SIM Provisioning**
  - Interoperable M2M
  - Remote SIM Provisioning Adoption

- **Future IOT Networks**
  - Evaluation of Low Power, Wide Area and Security Requirements

- **Industry Engagement**
  - Implementation of technology pilots and big data aggregation

- **IOT Business Enablers**
  - Operator Self Regulation Toolkit

**Vertical Ecosystem Engagement – Automotive, Transportation, Utilities and Health**

Email: connectedliving@gsma.com to track progress or join the Interest Groups

Visit www.gsma.com/connectedliving for more information on the Connected Living Programme, upcoming events & Industry Research

© GSMA 2015
Internet of Things - How did we get here?

**COSTS**
(compared to 10 years ago)
Sensors – 50% less
Bandwidth – 40x down
Processing – 60x down

**SMARTPHONES**
Gateway to IoT

**WIFI**
Everywhere – free or low cost

**BIG DATA**
IOT will unlock it

**IPv6**
3.4 x 10^34 addresses
YES, OF COURSE I REMEMBER THE 4 DIGIT SECURITY CODE ORANGE GAVE ME DURING A 5 MINUTE PHONE CALL...

...TWO YEARS AGO!
Security must exist because we need to

- Protect personal data
- Guard against fraud
- Protect the vulnerable
We don’t always like Security

Changing a “Necessary Evil” into an “Absolute Necessity”

IT RESTRICTS

IT IS COMPLEX

IT COSTS
Example - BMW
Spoofing the Cellular Network

- Rogue Cellular Base Station
- Connected Car
- Unencrypted, HTTP traffic

- Smartphone running Connected Car app
- Mobile Network Operator

- Friendly attack by ADAC – German Auto Association
- No customer data was disclosed
- Captured data from TCU <-> TSP

© GSMA 2015
How did they do it?

- OPEN SOFTWARE
  OpenBSC
- CLEARTEXT PROTOCOL TRAFFIC
  Relied on Network encryption
- IDENTIFY THE API UNLOCK
  Reversed engineered the code using IDA Pro disassembler
GSMA IOT Security Guidelines
Mobile World Congress Shanghai – 16th July 2015
Shane Rooney – Executive Director GSMA
What’s Next in the Connected Living Programme?

Building upon the recommendations contained in our “End-to-End Security for M2M & IOT” whitepaper the GSMA will now develop a public set of **IoT Security Guidelines**

- Must be **relevant** to IoT Ecosystem
- Use **existing technology** and standards
- **Security** (confidentiality, integrity, availability, authenticity) and **Privacy**
- Must be **industry agnostic**
**IOT Security Guidelines must influence the whole IOT Ecosystem**

Arrows show flow of ‘value’ within the system

Key entity in the ecosystem to influence is the Enterprise who wants to develop a connected product.

This entity sets the security requirements for the IOT service and its constituent parts and is the entity that is liable in the event of a security breach.
A set of IOT Security Guidelines centred the IOT Service Provider

Definition of IOT Service Provider

- The provider of IOT services working in partnership with a Network Operator to provide an IOT Service to an End Customer

Consider IOT Services that communicate over “managed” cellular networks (GSM, UMTS and LTE) and fixed networks.

- Considers security aspects of IOT Services that use local area and personal area networks.

- Consider all aspects of end-to-end IOT security – the people, the processes, the technology and the data exchanged.

- Not intended to create new IOT specifications or standards, but will refer to currently available solutions, standards and best practice.
**Guidelines Scope: What information should they contain?**

- Highlights the critical role of the IOT Service Provider in the IOT Ecosystem
- Overview of the key security risks and challenges for IOT Services.
- How the IOT Service Provider can mitigate risks by selecting partners who are competent in security and services and support standards based approaches.
- A set of ‘best practice’ security and privacy principles to be applied to the ecosystem partners during the entire IOT Service development lifecycle.
- Provides recommendations based on readily available systems, technologies and process that can be deployed today.

**CLP.14**
IoT Security Guidelines for IoT Service Platforms

- Operational best practices
- Cloud security configuration
- Security capabilities
- Authorisation and authentication
- Use of Virtual Machines
- Use Anti-Malware
- Load balancing and redundancy
- “Secure by Default”
- “Secrets” management tools

**CLP.13**
IoT Security Guidelines for IoT Devices

- IOT “Gateway” Devices
- IOT “End Point” Devices
- Secure local interfaces
- Certificate storage
- Physical security
- Embedded UICC
- Device Management
- Crypto capabilities

**CLP.12**
IoT Security Guidelines for Network Operators

- Subscription management
- UICC supply and management
- Communication channel security
- Authentication and encryption
- Network availability
- Roaming
- Operational and management best practice
- Backhaul security
- IOT device management
Who is involved?

Active project members thus far:

- If your organisation is a GSMA member – please join our project team and start engaging with the project today:
  - 7Layer
  - Anam Technologies
  - AT&T
  - BlackBerry
  - China Mobile
  - China Telecommunications
  - Cisco
  - Copper Horse Solutions
  - Deutsche Telekom
  - ETISALAT
  - Ericsson
  - Gemalto
  - Jasper
  - Morpho
  - NTT DOCOMO
  - VimpelCom
  - Orange
  - Sierra Wireless
  - Starhome Mach
  - Telecom Italia
  - Telefónica
  - Telenor Connexion
  - Telit
  - u-blox
  - Vodafone
  - Singtel

- If you are not a GSMA member - please help review our draft guidelines – to be circulated for industry review in ~ October 2015.
  - The industry review is your opportunity to ensure the guidelines ‘embrace’ all leading industry standards and best practices.
Points of Contact

SHANE ROONEY
- Executive Director – IOT
- srooney@gsma.com

IAN SMITH
- IoT Security Project Leader
- ismith@gsma.com

Further Information & Resources:
www.gsma.com/connectedliving