The Internet of Things: An Overview

Karen Rose
Senior Director, Strategy & Analysis
Internet Society
Setting the Scene

- About the Internet Society
- IoT Concepts & Drivers
- IoT Key Challenges
  - Security
  - Privacy
  - Interoperability
About the Internet Society
Who we are

Global not-for-profit organization, founded in 1992

*Independent* thought leader and advocate on issues impacting the Internet and its users.

Organization home of the Internet Engineering Task Force (IETF)
Our Mission

To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.
Our Global Presence

116 Chapters Worldwide
80,000+ Individual Members
143 Organization Members
6 Regional Bureaus
21 Countries with ISOC Offices
How We Work

We harness global expertise and work at the intersection of Internet:
• policy,
• technology, and
• development

2016 Agenda Focus:
• Promoting Trust in the Internet
• Connecting the Unconnected

If you care about the Internet, join us!
IoT Overview: Concepts & Drivers
What is IoT really?

One view, from McKinsey Global Institute:

- Despite the buzz, no single definition.
- Or agreed numbers, or categories, or taxonomies...
- Different emphasis on different aspects of the concept

- **Functionally:** The extension of network connectivity and computing capability to a variety of objects, devices, sensors and everyday items allowing them to generate/exchange data, often with remote with data analytic/management capabilities.

- **As Value:** *Data* & what can be done with it.

- **As a Vision:** The realization of a ‘hyper-connected” world.
  - This is why it matters.
  - This is why it’s hard.
Computers, Networks, and “Things”

“Machine to Machine” (M2M) (~1970s+)

Internet of Things Beginnings


Trojan Room Coffee Pot (first webcam) (1991)

Internet Toaster (1990)
If it's not new, why now?:
A Confluence of Market Trends

- Ubiquitous Connectivity
- Widespread Adoption of IP
- Advances in Data Analytics
- Computing Economics
- Miniaturization
- Rise of Cloud Computing
IoT Challenges
Key IoT Challenges

- SECURITY
- PRIVACY
- INTEROPERABILITY AND STANDARDS
- LEGAL, REGULATORY AND RIGHTS
- EMERGING ECONOMIES AND DEVELOPMENT
Key IoT Challenges

- SECURITY
- PRIVACY
- INTEROPERABILITY AND STANDARDS
- LEGAL, REGULATORY AND RIGHTS
- EMERGING ECONOMIES AND DEVELOPMENT
Security
Security Must be a Fundamental Priority

• Security is the most pressing and important IoT challenge for industry, users, and the Internet.

• Growth in devices increases the surface available for cyberattack

• Poorly secured devices affect the security of the Internet and other devices globally, not just locally.

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.
A Spectrum of Unique Smart Object Security Challenges

- Cost/Size/Functionality
- Volume of Identical Devices
- Deployment at Mass Scale
- Long Service Life
- No / Limited Upgradability
- Limited Visibility into Internal Workings
- Embedded Devices
- Physical Security Vulnerabilities
- Unintended Use & BYOIoT

See also IETF RFC 7452 Architectural Considerations in Smart Object Networking
Collaborative Security Approach: Developing Solutions in the Context of Principles

| Fostering Confidence / Protecting Opportunities | Opportunities for individuals, business, economy and and society will only be realized if there is confidence in the Internet, systems, and technologies (including IoT). |
| Collective Responsibility                   | No security threats or solutions exist in isolation. Requires collective responsibility, a common understanding of problems, shared solutions, common benefits, and open communication channels. |
| Uphold Fundamental Properties and Values     | Security solutions should be fully integrated with the important objectives of preserving the fundamental properties of the Internet and fundamental rights. |
| Evolution and Consensus                      | Security solutions need to be flexible enough to evolve over time & responsive to new challenges. Focus needed on defining agreed problems and finding solutions, including incremental ones. |
| Think Globally, Act Locally                  | Creating security and trust requires different players (within their respective roles / responsibilities) to take action and close to where the issues are occurring. |

See http://www.internetsociety.org/collaborativesecurity
Privacy
Privacy and IoT: Data is a Double-Edged Sword

- The data streams /analytics that drive the value IoT can also paint very detailed and intrusive pictures of our lives.
- Expands the feasibility / reach of surveillance and tracking.
- Redefining the debate about privacy issues
  - Can dramatically change the ways personal data is collected, analyzed, used and protected.
- Implications on our:
  - Basic rights
  - Sense of personal safety and control
  - Ability to trust the Internet and devices connected to it.
Different Dimensions of Privacy Challenges in IoT

- Breakdown of “Notice and Consent”
- Managing Across Many Devices
- Individual Preferences in Common Contexts
- Aggregation of Personal / Behavioral Data
- Cross-Border Data Flows
- Global Data Protection
- Discrimination
- Law Enforcement
Enhancing Privacy in IoT

- Strategies need to be developed that respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

- Traditional on-line privacy models may not fit.

- Adapting/adopting basic privacy principles, such as:
  - Transparency/Openness
  - Meaningful Choice
  - Data Minimization
  - Use Limitation
  - Among others..
Interoperability & Standards
I&S: Not Just a Tech Challenge, It’s a Market Issue

40% Interoperability is necessary to create up to 40 percent of the economic value generated by IoT

-- McKinsey Global Institute

Q: What are the greatest barriers inhibiting business from adopting the industrial Internet?

Source: World Economic Forum

- Lack of interoperability or standards
- Security concerns

<table>
<thead>
<tr>
<th>Region</th>
<th>Lack of Interoperability or Standards</th>
<th>Security Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>65%</td>
<td>60%</td>
</tr>
<tr>
<td>N. America</td>
<td>67%</td>
<td>64%</td>
</tr>
<tr>
<td>Europe</td>
<td>60%</td>
<td>72%</td>
</tr>
</tbody>
</table>
Interoperability / Standards Considerations

• Complex / Dynamic Service Delivery Chains and Use Cases
• Land Rush and Schedule Risk
• Proliferation of Standards Efforts
  • Industry coalitions, alliances, SDOs, proprietary development etc.
    • Can overlapping efforts be avoided without undue coordination overhead?
• Where is Interoperability Needed?
• Reusable Building Blocks
• Best Practices and Reference Models

Ultimately about advancing innovation and user choice
Closing Thoughts

• IoT is happening now, with tremendous transformational potential

• But the challenges must be addressed to realize the opportunities and benefits
  • Significant. Real. But not insurmountable
  • Solutions won’t found by simply pitting promise vs. peril

• It will take Informed engagement, dialogue, and collaboration across a range of stakeholders to find solutions and to plot the most effective ways forward.
Thank You

The Internet of Things: An Overview
Understanding the Issues and Challenges of More Connected World

http://www.internetsociety.org/IoT

Karen Rose
Sr. Director, Strategy & Analysis
rose@isoc.org