Introduction to the Web of Things

Interoperability across IoT platforms

Dave Raggett
W3C

北京, 11 July 2016
Massive Potential for the Internet of Things

- Smart Homes
- Wearables
- Healthcare
- Power & Environment
- Smart Cities
- Manufacturing
The Internet of Things – Bridging the Silos

Still very immature, and a long way to go

Lack of interoperability at the application level

Many platforms and associated standards
  - Addressing broad range of different requirements
  - End to end security challenging across platforms

Fragmentation and Silos are holding back the potential

Open or closed system?
  - Closed systems incentive: control
  - Open systems prompt: reduced costs and increased market size

Need for wide adoption of shared open standards
The IoT Standardisation Challenge

- AIOTI WG03 IoT Standardization landscape (and still extending)
What we want to avoid ...

How standards proliferate:
(See: A/C chargers, character encodings, instant messaging, etc)

Situation: There are 14 competing standards.

14?! Ridiculous! We need to develop one universal standard that covers everyone’s use cases. Yeah!

Soon:

Situation: There are 15 competing standards.
Web of Things – Inter-Platform standards for interoperability

The Web will enable a transition from costly monolithic software to open markets of apps
Analogy with early days of networking

Before the Internet, there were many non-interoperable network technologies

- IP made it simple to interconnect networks and create interoperable services independent of the network technologies
- The Internet grew exponentially as the opportunities were realised
- Likewise for the Web which took over from isolated information services

Direct analogy with today’s IoT silos and their lack of interoperability

- The Web of Things is the equivalent of IP for semantic interoperability and end to end security
- The Web of Things will enable explosive growth as the barriers to interoperability are torn down
The Web of Things

- **Simplifying application development by decoupling the underlying protocols**
  - By analogy to the cross platform sockets API for the Internet Protocol
  - Making it easy to write apps that can be easily ported to different platforms

- **Enabling interoperability across different platforms with standardised metadata**
  - Describing the interfaces exposed to applications
  - Describing the communication and security requirements for accessing things
  - Describing the semantic models and domain constraints, enabling
    - shared meaning across communicating parties
    - validation for robust operation
    - search and composition of services
Web of Things

Applications act on software objects that stand for things
- Local “things”
- Remote “things”

Rich descriptions for every “thing”
- Each thing has a URI for its name
- This provides access to its description
- Ontologies that describe “things”

Things don’t need to be connected
- Abstract entities and unconnected physical objects
Scalability

Web of Things servers can be realised at many scales from microcontrollers to clouds

**Home Hub:** home/office server for access to smart home and wearables, running behind firewall

**Micro-controller:** resource constrained, IoT devices or gateways, CoAP, running behind firewall

**Smart Phone:** personal server for access to smart home and wearables

**Cloud-Based:** highly scalable server for many users, devices and working with big data
The Web of Things in the Home

- Ambient or battery operated IoT devices
- Gateway (apps)
- Powered, multi-protocol
- Cloud based Services
- Browser for HMI
- Firewall
What kinds of metadata do we need for this?

- Thing lifecycles, data and interaction models
  - As exposed to the applications

- How to interoperate with another platform?
  - Mapping from thing descriptions to platform specific protocols
    - IP address and port for IP based protocols
    - Paths for REST based protocols such as CoAP & HTTP

- What communication patterns to use?
  - Push, pull, pub-sub, peer to peer
  - Real-time requirements
  - Transactional robustness & rollbacks
  - Multiplexing and buffering
  - Sleepy ambient & battery powered devices

- Semantic models of things and their constraints
Data & Interaction Models

Must be rich enough to cover broad range of use cases and platforms

- Properties, actions and events carry values
  - Actions are asynchronous and can be passed a value, and may return a sequence of values

- Values as basic types
  - Null, true, false, numbers, strings

- Compound values
  - Arrays
  - Sets of name/value pairs
  - Things
  - Streams

- Integrity constraints
  - On single values, e.g.
    - min/max, integer/float
  - Across multiple values
  - Cardinality constraints
  - Need for path expressions

- Complications
  - Proxy chains
  - Early and late binding
    - Partially defined types
  - Cyclic dependencies across things
  - Software dependencies
    - Metadata constraints (versioning)
Semantics

- Needed to ensure that platforms share the same meaning for the data they exchange

- Enables richer validation against domain constraints

- Simple approach is to define semantics as part of the system specifications
  - But this makes it easy to lose track when data is stored and passed to other systems, or when a system evolves to address changing requirements

- Better approach is to tag data as belonging to an ontology that describes the relationships between concepts in a machine interpretable way
  - What kind of a thing is it?
    - e.g. a temperature sensor
  - What are the domain constraints?
    - temperature sensors must describe their physical units, which must be from the set {Kelvin, Celsius, Fahrenheit}
    - Other ontologies could describe the location of the sensor and what it is measuring
Ontologies allow information to be exchanged meaningfully in a way that is independent of the data formats used for its transmission.

Ontologies further allow for checks that the information is consistent with the domain models.

This can cover richer constraints, e.g. temporal constraints across actions and properties.

W3C has a suite of standards for the Semantic Web and Linked Data:
- RDF, XML, SPARQL, RDF-S, OWL, RIF, JSON-LD, RDF in CSV, DCAT . . .

Enable semantic based search and composition of services:
- Ensure that compositions will use interoperable services.
Data Security and Privacy
IoT Security Should Worry Us All

- Breaches of privacy
- Cybercrime
- Physical safety in the home, across the city and within businesses
- Threats to national infrastructure
- Looming risks of cyberwar
Unique Challenges for IoT Security

- IoT relies on microcontrollers with limited memory and computational power
  - This often makes it impractical to implement approaches designed for powerful computers
  - This in turn requires constrained IoT devices to be hidden behind secure gateways

- Threats based upon gaining physical access to IoT devices

- How to bootstrap trust and security, and ways that this can unravel

- Evolving technology
  - More powerful Systems on a Chip (SOC) embedding hardware security support
  - Elliptic Curve Cryptography with reduced computational demands

- Anything that is exposed to the Internet must be securely software upgradable

- User experience must be good enough to avoid becoming a weak link in the chain

- The necessity of keeping up to date with security best practices
The Challenges for the IoT and Big Data

- Lots of sensors will generate a vast amount of data
  - API Research estimated 200 exabytes in 2014 and 1.6 zettabytes in 2020
  - 90% is currently processed locally, although this varies by domain

- This creates a greater volume of sensitive data, increasing the risk of
  - Data and identity theft,
  - Device manipulation,
  - Data falsification
  - IP theft, server/network manipulation, etc.

- Impact of introduction of data consolidation and analytics at network edge
  - Cisco, HPE and others
  - App platforms in the cloud or at the network edge will be targets for attacks
Enabling Data Security for the Internet of Things

- Transport and app layer encryption
  - TLS and DTLS for encrypting data transmitted over the Internet
  - Plus app layer encryption for greater security where needed
  - Secure key exchange algorithms over unsecured channels

- Authentication and Key management
  - IoT devices need to check that the server is who it says it is
  - Servers likewise need to check this for IoT devices
  - Asymmetric Public/Private key pairs vs Symmetric keys
  - Tamper resistant storage of keys and certificates
  - Challenges for provisioning services
Authorisation – Determining Who Can Do What

- Authorisation rules
  - Authentication of the data recipient
  - Simple form of rules as access control lists
  - More general rules with complex conditions

- Capability based security
  - A capability is communicable and unforgeable token of authority
  - The token is associated with a set of access rights

- IETF work on ACE and JOSE
  - ACE: access control in constrained environments
  - JOSE: JavaScript Object Signing and Encryption

- Relationship to models of trust
  - Prior agreements between two parties
  - Attestations by trusted third parties
Privacy and the Internet of Things

- The IoT has the potential to provide huge and unprecedented amounts of personal information
  - This information may last indefinitely
  - Risk of abuse by individuals, criminals, companies and governments
  - Sense of intrusion into your personal space
  - Fear of harm due to disclosure of personal information

- Strongly identifying information
  - Your address, data of birth, sexual orientation, ...
  - Principle of data minimisation – high cost to companies for handling personal data securely
  - Privacy policies determining what purposes data can be used for, and for how long

- Weakly identifying information
  - When sufficient such data is combined this can uniquely characterise you
  - Companies need to provide privacy policies on how they handle such data

- Need for adhering to best practices to avoid reputational damage to companies
  - Including regulatory requirements
The IoT and the Web

- Web technologies are increasingly important for the IoT
  - Web protocols like HTTP
  - Semantic descriptions based on RDF
  - HTML5 and the Open Web Platform for human machine interface
- The Web security model and its relationship to the IoT
  - Access rights for web apps are scoped to app’s origin
  - The Web is moving to encrypt all communication
  - We’re preparing to transition the Web from passwords to public key crypto
    - Users authenticate to the browser, and browser authenticates to the website
- For the IoT, the user (owner) isn’t around at the time the device needs to authenticate itself to a service
- We therefore need a way for users to authorize the device in advance
  - This is a form of trust delegation, and introduces the need to authenticate users as well as service providers
Web of Things
Activity
W3C is chartering a Web of Things Working Group to develop initial standards
- This group is expected to launch later this year

W3C Web of Things Interest Group is re-chartering
- Expected to boost its work on reaching out to industry alliances and SDOs
- Interoperability tests across platforms using open source implementations
- Further joint papers planned on security, privacy and requirements for open markets of services

Plans for an IoT on the Web Business Group
- Focusing on business and policy level requirements across domains
- Including what’s needed for agile process for developing and standardising models and vocabularies
W3C Web of Things Interest Group

Workshop in Berlin (June 2014)
- Launch of Web of Things IG in 2015
- Chaired by Jörg Heuer, Siemens
- Task forces
  - Thing descriptions
  - APIs and protocols
  - Discovery and provisioning
  - Security, privacy and resilience
  - Communications and collaboration

Strong emphasis on implementation experience
- Demos and plug-fests
- Helps to build a shared understanding

Montreal Face to Face, 11-13 April 2016
Members of the Web of Things Interest Group
Reaching out to industry alliances and SDO’s to drive convergence to unleash the potential

- Plattform Industrie 4.0
  - Especially the “semantics” subgroup
- Proposed German Smart Home Initiative
- Industrial Internet Consortium
- Open Connectivity Foundation
- OPC Foundation
- IETF/IRTF
- BSI & Hypercat
- oneM2M
- GSMA
- AIOTI
Web of Things Working Group

The Interest Group (IG) is working on
- Use cases, requirements, technology landscape and plans for launching working groups (WG)
- IGs prepare the ground for standards but don’t develop standards
- WGs are chartered to develop standards (W3C Recommendations)

We’re collecting ideas for a Working Group including
- Horizontal metadata vocabularies (things, security, communications)
- Serialisations of metadata, e.g., as JSON-LD
- APIs and bindings to specific protocols and platforms in collaboration with the platform owners

Web of Things Working Group to be launched late 2016
The Bottom Line

The Web is essential for realizing the full potential of the IoT

The Web provides a unifying framework for semantic interoperability

The Web acts as a global marketplace for suppliers and consumers of services
Work with us to build the Web of Things!

For more information on W3C see:

www.w3.org
Web of Things

What, why, how, actions
What is the problem to be addressed?

Fragmentation of the IoT into many non-interoperable platforms

Why is it important?

Solving this will enable exponential growth as we saw with the Internet and the Web
- The network effect: Metcalfe’s law

How it is to be solved?

- Inter-platform standards that play an analogous role to IP for connecting previously incompatible networks
  - Decoupling applications from protocols
  - Enabling different platforms to interoperate
  - Complementing, not competing, with platforms

What action are we seeking?

- Commit to join W3C & assign staff to participate in Web of Things groups
- Ensure your company is in the driving seat for the open IoT
What is the problem to be addressed?

Difficulty of creating services spanning different platforms due to a lack of semantic interoperability and a mismatch of assumptions around trust and security.

Why is it important?

Solving this would enable exponential growth in services like we saw for IP and the Web.

How it is to be solved?

Inter-platform standards defining an interlingua for metadata, and shared assumptions in respect to end to end security across different platforms.

What action are we seeking?

Active collaboration on integration with the Web of Things and alignment of marketing messages.
Engineers and Developers

What is the problem to be addressed?

- Fragmentation of platforms and IoT technologies, and high cost of integration with a piecemeal approach
- Barriers for semantic interoperability and end to end security

Why is it important?

- Simpler, faster, more flexible application development
- Leveraging existing services and communities in the Web ecosystem
- Be part of the next big thing, strong growth in job opportunities

How it is to be solved?

- Open standards for Web based abstraction layer, complementing existing platforms and standards, and enabling platforms to interoperate securely

What action are we seeking?

- Joint work on experimental implementations that explore what it means to integrate with the web of things – help to create evaluation kits, and spread the word
- Joint work on white papers to forge a shared understanding across companies, alliances and SDOs