Monohm Position on WoT

ABSTRACT

The emerging Web of Things (WoT hereafter) subset of IoT incorporates a set of requirements that, while modest by the wider IoT scheme of things, presents challenges to currently accepted Web behavioural set.

Monohm believes that most of the challenges presented by emerging WoT requirements can be met using existing standard protocols.

SCOPE

This document proposes that protocols and mechanisms which are currently accepted in conventional home LAN and wider Web deployments be suitable for adoption in a WoT environment.

This document is intended to suggest a baseline for minimal interoperability rather than be an extensive treatment on the subject.

This document specifically refers only to LAN-based communication.
This document specifically refers only to IP-based communication.
This document only briefly refers to WoT related security concerns.

USE CASES

1. I want to increase or decrease the temperature of my house.
2. I'm leaving my house and want to ensure that my appliances are in a safe state.
3. I'm approaching my house and want to open my garage door.
4. I want my curtains to close when it becomes dark outside.

DISCOVERY

The Web is generally point to point. Endpoints ask other endpoints how to locate further endpoints. Every reachable endpoint is assumed to have a catalogue entry which is available via an efficient and timely mechanism.

A collection of heterogenous things bears almost no resemblance to the conventional web. Devices routinely appear and disappear from view. Keeping a catalogue of endpoints is considered a sufficiently laborious, continual, or technical task that it simply won't be done.

Therefore, to discover these devices in order to communicate with them, we need an alternative to conventional Web mechanisms.

Fortunately, in the last decade or so, a de facto standard has emerged in the LAN discovery space. Apple's Bonjour provides an efficient mechanism for dynamically locating devices via a creative use of DNS over a multicast ring. This protocol is a widely ported open source standard, and is in current daily use in millions of home and office environments facilitating discovery of all kinds of devices.

Monohm proposes multicast DNS as a standard for WoT device discovery.

SPECIFIC INTERACTION

One of the factors differentiating WoT from IoT is that end user interaction is a primary consideration. Given that a likely deployment environment for a good proportion of WoT devices is the home, the requirement for easy configuration and convenient operation is clear.

Device manufacturers will likely want to provide a quality branded experience to accompany their product, without the implementation burden that goes with producing and maintaining clients for all current major platforms.

Once a device's address is known, then traditional Web protocols become appropriate. The Web has long had a standard and reliable mechanism for providing platform neutral interaction.

Monohm proposes that device-specific UI be facilitated in HTML, served from the device itself via HTTP. In addition, Monohm proposes that any required asynchronous or streamed functionality be implemented with WebSockets.

GENERAL INTERACTION

One of WoT's aims is to avoid an exponential explosion of software resulting from a rapidly growing market of devices. Therefore a likely requirement in any upcoming WoT standardisation portfolio is that devices' capabilities be determined opaquely - that is, without any specific knowledge of a device's maker or function.

Once a device's address is known, then traditional Web protocols become appropriate. Opaque retrieval and update of device properties via standard protocols and encodings permit clients of all types to easily play in the space.

In addition, opaque interaction implies that the implementation of any specific interaction is optional. Once sufficient information regarding the device's properties is communicated, then a user interface for interacting with the device can be generated.

Monohm proposes that device properties be retrieved in JSON format via HTTP, and that properties be updated via HTTP parameters.

SCRIPTED INTERACTION

If devices can be found by a standard protocol and their properties’ values managed similarly, then it follows that interactions between them can be easily automated. If all WoT devices speak the same language, then for the price of a simple user interface, powerful rule systems which connect disparate collections of them can be authored and maintained by end users.

CONFIG vs PROPERTIES

Under the scheme proposed by Monohm, the set of properties owned by a device is divided up into two categories, referred to as “configuration” properties and “properties” properties. The “configuration” set refers to the configuration of the device itself, such as its name, advertised type, and port number, which are mostly standard across device types. The “properties” set refers to data items pertinent to the device’s mission, such as latitude and longitude for a location sensor.

The scheme divides these due to their conceptual difference, physical implementation, and perceived security differences. Configuration might be held in non-volatile storage, whereas properties reflect the state of the device’s sensors. Likely, the configuration contains properties which are neither readable nor writable after initial device installation, whereas property values might even be public.

ARBITRATION

One significant outstanding question as regarding WoT deployments has been whether participants in the community find each other or via a “hub” node which facilitates discovery (among other functions). Each approach has its benefits and issues. On the one hand, a peer to peer network has less configuration overhead and does not have a single point of failure. On the other hand, a hub permits centralised permission management, and can also serve as a gateway to the WAN.

Monohm proposes that devices be capable of both topologies, ie that the need for centralised management or security not be mandated.

SECURITY

The subject of WoT security is a necessarily important and complex one. There is no one correct strategy for such a potentially large distributed homogenous interconnection of devices with a wide ranging set of use cases, privacy concerns, and security requirements.

However, if Web-style transports are deployed in a WoT environment, then Web-style security can be layered upon them. This transparently enables such accepted security paradigms as SSL, Secure-DNS, .htaccess, and OTP.

PASTPROOFING

Currently, most browser environments are not capable of directly dealing with the UDP protocol which is required for participating in MDNS-based service discovery. Some browsers have upcoming UDP facilities which require the client application to be packaged in a specific way, while others have no promise of UDP facilities.

Monohm proposes the use of an HTTP proxy in these environments.

REFERENCE IMPLEMENTATION

Monohm have produced Sensible, a reference implementation demonstrating the fundamentals of its proposed WoT platform.

Sensible incorporates --

- multicast DNS client and server
- HTTP server
- HTTP proxy for non-UDP compliant platforms
- application wrapper providing easy service advertisement and hosting

Sensible runs on Node.js, Firefox OS, and Chrome OS.