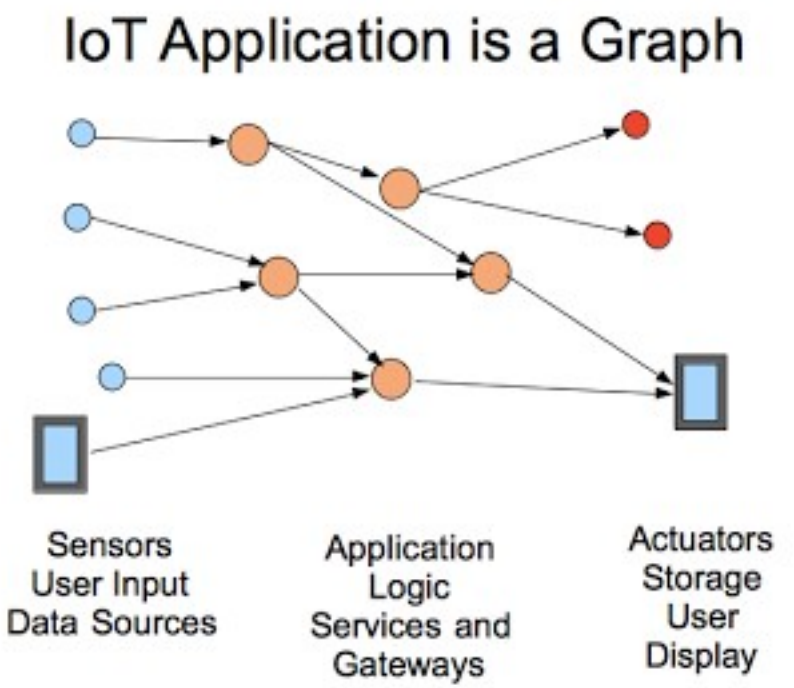
The Personal Object: User Control of Identity, Resources, and Experience on the Internet of Things

Michael J. Koster
January 20th, 2013

User Agency on the Internet of Things

The Internet of Things connects people and things together with software.

The most recent article on Open Infrastructure describes the Internet of Things application as a graph which contains sensors, actuators, and user interface devices at the edges and rules, triggers, and other application logic at the nodes, executing in the sensors themselves, in gateways, and in cloud services. These application graphs are built and customized according to user intentions and user context.



This article discusses the idea of user agency on the Internet of Things; users will need ways to express their intentions and constraints to the system in the management of IoT resources and devices owned and controlled by the user.

Scalable, granular, and simple user authentication and control

Users and creators are roles that exist at all levels of the system. Users create application graphs based on intentions and context. Creators are users of a platform, and give users tools and systems with which to customize their own experience.

Users share data with other users, with service providers, with everyone, or with no one, as needed, in a granular way, to compose these application graphs. Users also import data shared out by others to compose into their own application graphs.

Clearly, the ability of users to control and manage their resources will become a limiting factor, if current authentication and control mechanisms are used. Passwords and user accounts using existing permission schemes will place severe limits on the granular scalability and robustness achievable for the future Internet of Things.

It has become clear that a system of user control for the Internet of Things will need to be built into the basic access mechanism of the IoT platform and APIs from the beginning, rather than something added on. It's also clear that the design should be based on user intentions and user control as underlying principles.

User control of identity, resources, and experience on the Internet of Things

From this a basic requirement emerges. For an effective, scalable deployment of the Internet of Things in a way that respects users intentions, we need to build in a system that places the center of control with the user. As a start, we propose to build affordances that give users control of their **identity**, their **resources**, and their **experience**.

The stability and robustness of IoT applications depends on a stable base of **identity** from which users can be confident that only their intentions are being implemented in their application graphs. User identity must be consistently maintained across multiple service providers, in a way that is also portable and replicable across identity platform providers. This is necessary in order to achieve an ecosystem that allows users to choose services and providers that best support their needs.

It is important that users have control of both the identity itself and of the platform used to provide it. This provides a base of assured user agency and retention of user resources and context in the face of changing business conditions. It also allows presentation of a free market choice to users.

User **resources** (data, sensors, "things", virtual objects) must be accessed under user control or by entities delegated by the user to access the resources. Control needs to be delegated on a fine grain basis so that the user can maintain a "need to access" policy for individual data elements, e.g. their height and weight but not their cholesterol count or blood pressure, and perhaps for a limited time period or for a one-time access.

The control of resources thus needs to be linked to user identity, and given out only under user authority. There needs to be ways in which users specify their intentions for resource control and sharing easily and unambiguously, while taking into changing account user context and user situations.

Users must be in control of their **experience**: to create IoT application graphs based on their own intentions and context, and to choose or compose whatever user interface is appropriate. Users intentions and context will direct the composition of user application graphs. Semantic description frameworks with discovery and linkage mechanisms allow user intentions to be determined through context and unambiguously applied.

For example, a user may have a graph describing their house such that a generic energy management ontology can be applied to control lights and heaters, further customized by adding knowledge of user preferences to the graph. It should be easy to "tinker" with a generic template to customize the user experience.

System based on knowledge and transparency

The Internet of Things protocols, APIs, and platforms need built-in methods to apply user intentions to resource access control. The idea is to build in mechanisms that allow users to define their intentions and apply them to the information graph of the system, and for the API to only be capable of resource interactions that are consistent with user/owner intentions.

A system of shared secrets and passwords for accounts and login mechanisms won't work for the scale and granularity of the IoT. This system barely works for the web today, and is being replaced by lower friction systems like Oauth.

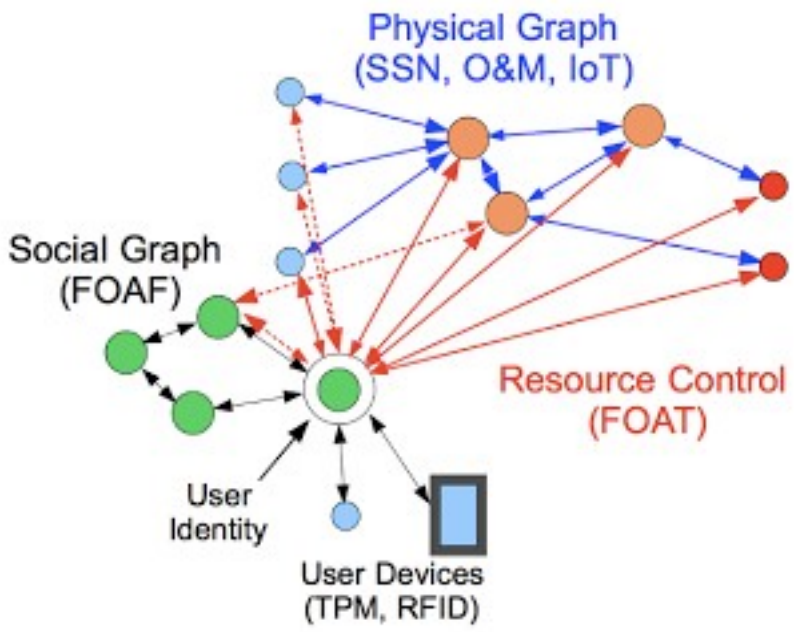
We propose to base user authentication and resource control on strong knowledge of graph relationships. This allows the user's intentions to be plainly known throughout the application graph, and can plainly expose attempts to falsify credentials or manipulate the system.

We can use the social graph to authenticate users, by using the unique set of graph connections that a user has to other users and to the objects they own. These graph connections can be validated by checking links back from multiple graph objects at different locations. The concepts that define relationships between people are defined in the Friend Of A Friend (FOAF) Ontology

We can also build a resource graph consisting of Smart Objects connected to services and other Smart Objects, based on the Smart Object, Sensor net, and related IoT ontologies, and the Smart Object API.

What's needed now is the mechanism to connect the two graphs, such that users are authenticated by not only their social relationships, but also their verifiable connections to "things", for example an RSA key or RFID badge, or both. Connecting the social graph to the

physical graph will also allow direct expression of the authenticated users intentions within the application graph.



Resource control will be defined by the graph linking users to their resources and defining predicate concepts that, for example, define that a particular entity in the user's FOAF graph "may observe" a particular resource under the user's control. These concepts can be defined in a "Friend Of A Thing" (FOAT) ontology. The idea is to allow resource owners to precisely define the resources to be shared and the constraints, e.g. time limit, number of observations, on the sharing.

Personal Object

We believe that the only way to accomplish this responsibly is to give users full control of their social and physical graphs. For this we need a provider-neutral identity API and platform based on open internet standards. We propose an Internet Personal Object, or Personal Object, to be constructed using a Linked Data API (Smart Object API or generic Linked Data) to hold user's social graph connections, preferences, and other identity information.

The Personal Object is essentially a Smart Object that represents a person's identity and some of their preferences and intentions, from which users can add graph relationships to define access control for Smart Objects and other internet resources under control of the user.

We propose to create a Personal Graph API, using the Smart Object API resources and service layer, to create a Personal Object. This API, along with the extended FOAF and FOAT ontologies, would be used to create strong identity-control graphs between owners, their delegates, and the things they control.

Personal Cloud Instance

There is another area of user agency to be considered in the deployment of the Internet of Things. Users get benefits in mobile accessibility, and may gain something in redundancy and professional data management, by keeping our information resources in proprietary cloud application services, but what is lost is control. We don't have any guarantee of continued access to our data, and we depend on a proprietary platform that we can't replicate in order to interact with our data anyway. If we can create or purchase software, it will be locked into a proprietary platform.

With cloud computing we have the opportunity to provide a new level of robustness and user control that couldn't easily be achieved through hard drives on PCs. We need to create a new class of platform-as-a-service that gives the user control over their environment and applications, much the same as the PC environment provided. These services can be linked in redundant fashion with multiple points of service, including local hardware gateways.

For ultimate user control, we propose a personal cloud service, for example an Amazon micro instance, that can host the personal object in a vendor-independent way. This can be updated through various social graph APIs in order to keep up to date with changes in one's social network.

We propose a basic user-customizable Open Source tool for users to manage their social and physical graphs; sort of an Internet of Things "address book". The user's social graph connections (of those who mutually choose to participate) are maintained in FOAF, and the physical graph connections are maintained using FOAT. The tool would allow broad preferences to be established, including cultural context, with personal customization.

PCaaS

A platform based on Open Source software can be built and deployed as a standard OS image that has all the necessary services pre-configured. There could be multiple instances in different cloud providers managed as redundant copies of a user's Personal Object. The cloud platform would also include instances of Smart Object services for user-created IoT application graphs and graph elements, and be able to run IoT applications on behalf of the user in the personal cloud service.

This framework would extend to physical IoT gateways, providing user control all the way to the IoT endpoints. IoT applications may then be distributed easily across cloud services and into local gateways.

This Personal Cloud Service can interact and share with other proprietary services and walled gardens, etc., but users must have a stable information base that is under their control from which other relationships can be managed. This will form a stable sub-structure for user agency on the internet.

How to enable users to control their identity, resources, and experience on the Internet of Things:

1. Create a personal social and local resource graph that users have control over, using an Open Source freely available platform and linked data API

2. Create a Personal Object that stores the resource graph, and additionally manages the users preferences and intentions as policies. Create and manage links from the social graph to the physical graph using a freely available Open Source tool such as an "IoT Address Book".

3. Host the Personal Object in a Personal Cloud service that is under control of the user. Use Open source stacks and tools for all essential infrastructure.