On Access Control in the Internet of Things

Jan Janak, Hyunwoo Nam, and Henning Schulzrinne
Columbia University

February 15, 2012

Abstract

Existing authorization frameworks, commonly used to control access to online services and nodes in the Internet, are role based and not suitable for IP based networks of sensors, actuators, and controllers. First, the identity of the user is established and then his or her access privileges are determined from the user's role within an organization. A light actuator, for example, does not need to know the identity of the switch, as long as the switch can prove that it is located in the same room.

Even ordinary actuators, and controllers in the real world are subject to access control restriction. There, authorization decisions are usually made based on a number of attributes claimed by the controller, not identity. We are designing an attribute based authorization framework for IoT devices to be used to implement common access restrictions that had been present in those actuators and controllers before they were upgraded and connected to the Internet. We want to be able to keep such devices connected to the global network, while preserving common access restrictions (now implemented in software).

1 Introduction

Imagine a hypothetical future campus where all the devices have been connected to a common network and use standard Internet protocols to communicate. An electronic key (in form of a smart phone) sends a command to the door lock to open the nearby door. A light switch controls lights in a room over IP. The light lets any device to control it as long as the device is located in the same room. To let a visitor inside a building, you will send them a one time access code so that they can use their smart phone to open the door. Facilities could adjust air conditioning and lights in rooms remotely when approved by current occupants of the rooms.

As result of opening up access to physical devices, new online services start to emerge. Startups will sell power saving plans online, monitoring sensors and adjusting actuators in homes remotely. Standardized interfaces allow them to compete on algorithms and large scale optimizations, not on exclusive access. Online services will offer personalized assistance with all kinds of routine, daily tasks, involving physical devices, communication technologies, and other online services.

All the scenarios mentioned above would be possible if we manage to solve one important problem. The problem of access control in open networks of sensors, actuators, and controllers. When we take ordinary physical devices and connect them to the Internet, we remove a number of access restrictions that have been present in those devices before. Some of them

are obvious; most people would agree that letting strangers open their front door over the Internet is probably not a good idea. Others are more subtle and often applied without giving it much though. Do you remember searching for a light switch in that dark room? Why wasn't the light switch installed on the outside, next to the door?

We strive to design and implement an authorization framework for networks of actuators and controllers that would allow us to describe authorization policies and implement fine-grained access restrictions to individual sensors and actuators. Having such an authorization framework in place would allow us to reap some of the benefits of keeping the sensor network connected to the global Internet, such as the possibility of integration with 3rd party online services and applications running in the cloud.

Our goal is to implement an attribute based access control system which can, unlike role and identity based systems common in online Internet services, take into account various attributes of the controller and not just its identity. Our authorization framework will make it possible to implement access restrictions to sensors and actuators based on date and time, location, proximity, invested effort, role, identity, etc.

We will use the framework as part of our ongoing effort to replace all kinds of sensor and actuator devices, such as light switches, door locks, power outlets, environmental sensors, AC units, with their Internet enabled counterparts.

2 Related Work

Most existing authorization frameworks for computer networks and online services are role based. First, the identity of the user is established and then his or her access privileges are determined from the user's role within an organization. That applies to most of existing network authorization systems and protocols (RADIUS, LDAP, IPSec, Kerberos, SSH). Online applications and services commonly rely on HTTP cookies stored in a user's browser after their identity has been verified. Although individual authorization systems may differ in how they establish users' identity or how they map the identity to roles and access restrictions, the mechanism always involves identifying the user.

Role based access control systems are not suitable for devices in the Internet of Things. There, the identity of individual device may not be known or may not matter. Access control is typically based on other criteria, such as location, proximity, invested effort, and others. To implement even the simplest common scenario, such as that a device may control the light in a room only if it is located in the same room, we need a more generic attribute based access control system. The Extensible Access Control Markup Language (XACML) can be used to describe attribute based access control rules. OAuth is an access control system for applications (not users), but requires that applications prove their identity by submitting tokens.

To the best of our knowledge, the means of claiming properties by devices and using that information for access control in common Internet of Things scenarios have not been investigated.

3 Our Approach

We are building an authorization framework for Internet Protocol (IP) based networks of sensors, actuators, and controllers (referred to as devices). In our model scenario the devices connected to the network represent ordinary devices commonly found in homes, offices, or on university campuses. Such devices can include: light switches, lights, door locks, door bells, keys, phones, projectors, remote controls, TVs, etc. We assume all such devices have been connected to a common network and can communicate with one another using standard protocols.

We will create a formal model for each the following environments: home, small office, university campus. We will use the models to understand the types of devices used, access restrictions applied, and people (and their roles) involved in interactions with those devices. Each model will describe:

- Types of sensors, actuators, and controllers used in the environment and their properties.
- Access restrictions applied to sensors, actuators, and controllers in the selected environment.
- People interacting with the devices, their relationships and roles (facilities, lab manager, parent, room occupant, etc.)
- Type of information we need to gather about controllers to make authorization decisions (location, proximity, identity, role, etc.)

We will express access restrictions identified in the formal model in form of attribute based access control rules. One of our design goals is to make such access control rules reasonably easy to understand and create, hence we will try to make language intuitive enough to be used by non-programmers.

Assuming all the devices have been connected to an IP network and can freely communicate with each other using standard protocols (HTTP, CoAP, or SIP). We will create a reference network architecture that would allow us to apply the access restrictions from the model to the devices. If a light in a room could have been controlled only a switch in the same room prior joining the Internet, we want the same restriction continue to apply, no matter how many other devices claiming to be light switches can talk to it. We want to implement such restrictions without having to cut the devices off the Internet completely, e.g., by placing them behind a firewall or inside a walled garden.

Finally, we will implement the system and deploy it on the network of sensors, actuators, and controllers we have been building on our campus. Our goal is to have all kinds of devices in a part of our campus connected to the common network with access and control restrictions implemented in software.

Having such network would give us a unique opportunity to experiment with various ways of automating common daily tasks involving the devices as well as use devices like smart phones to control everything from door locks to lights and projectors.