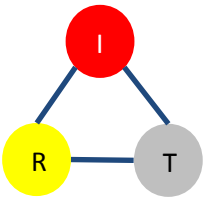
IAB Workshop on Smart Object Security
Paris, March 2012

Access Control for Smart Objects

Jan Janak, Hyunwoo Nam, Henning Schulzrinne

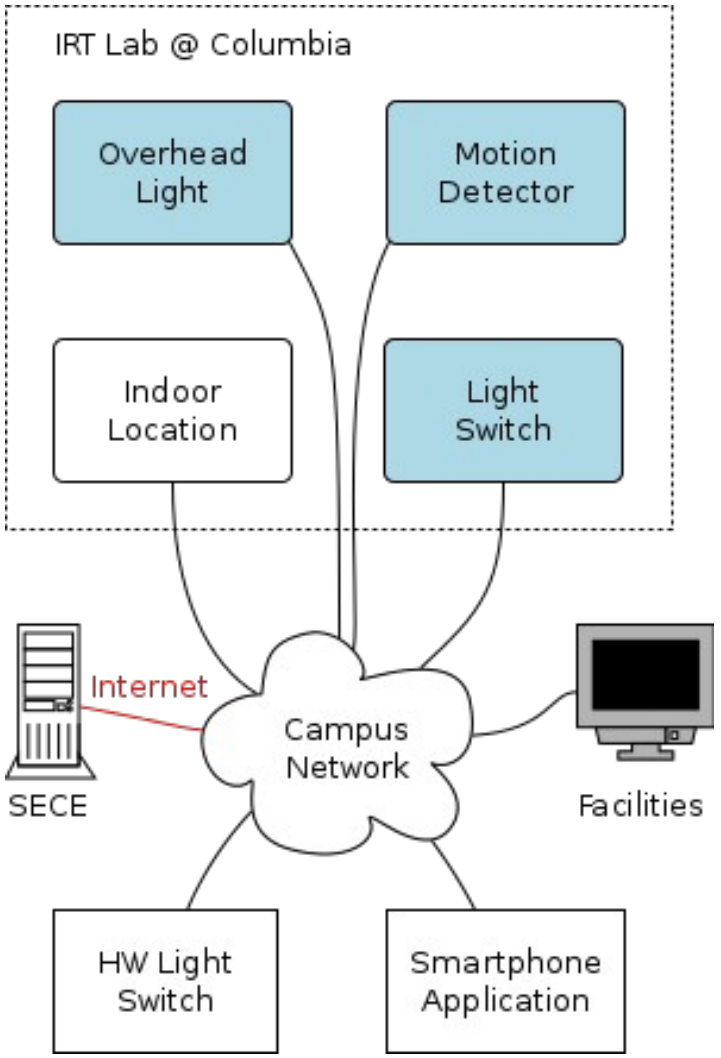


Internet Real-Time Laboratory

Columbia University

This work is sponsored by AT&T Research.

Office Automation with Smart Objects

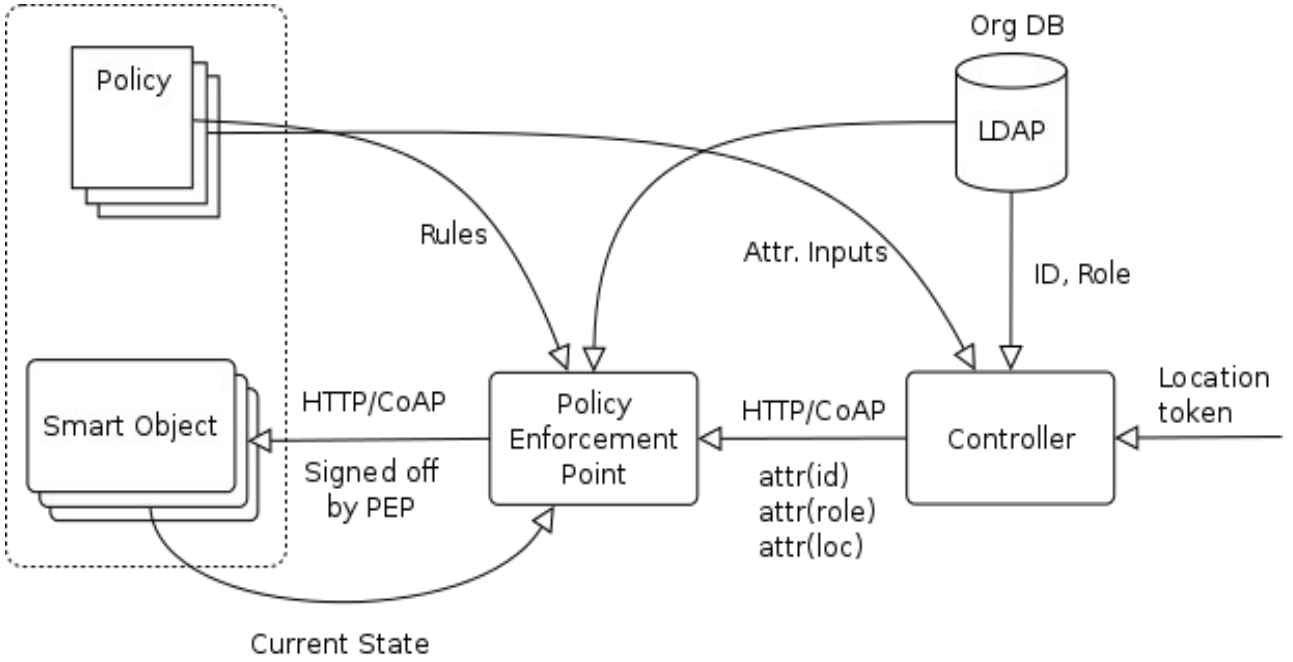


- Multiple controllers
- Need to specify and enforce policy
- A variety of inputs
- Provide reasonable default policies for SO

Overhead Light Policy:

```
id=="irt_switch" or
location=="irt_lab" or
(action=="OFF" and app=="SECE") or
Group=="Facilities"
```

Initial System Architecture



- Controllers sends requests with a set of attributes
- PEP verifies attribute values and signs the request.
- Policy documents specify conditions and required attributes.
- Each Smart Object type has a default policy that can be overridden.

What Makes it Complicated?

SO Candidates

- Lights
- Motion detectors
- Door locks
- Wall sockets
- Towel dispensers
- Fire alarm buttons
- Elevator controls
- Phones
- Indoor location

Policy Inputs

- Identity
- Date and time
- Proximity
- Geo-location
- Effort (press 3x)
- Result of a vote
- Current state of SO
- Organizational role
- Randomness

Open Questions

- How do we describe and enforce access restrictions applied to Smart Objects?
- What protocols can we use to implement attribute-based access control?
- Mapping of credentials to CoAP/HTTP requests?
- Where is policy enforced? How do SOs learn the outcome?
- Default policy from SO manufacturers?