Wireless Network Security
Spring 2016

Patrick Tague

Class #20 – IoT Security & Privacy

Class #20

- What is the IoT? …the WoT?
  - **IoT ≠ Internet, WoT ≠ Web**

- Examples of potential security and privacy problems in current and near-future IoT usage scenarios

- Architectural changes that may address these issues

The Internet of Things is … ?

- What kind of things are we interested in connecting to the internet? My computer, laptop, and phone are all things…has the IoT been around for 40 years?

- If I put a WiFi chip in a sensor and stick the sensor on the wall, did I just create the Internet of Things?

- When my Nest thermostat controls my heater using data from the cloud, is that the Internet of Things?

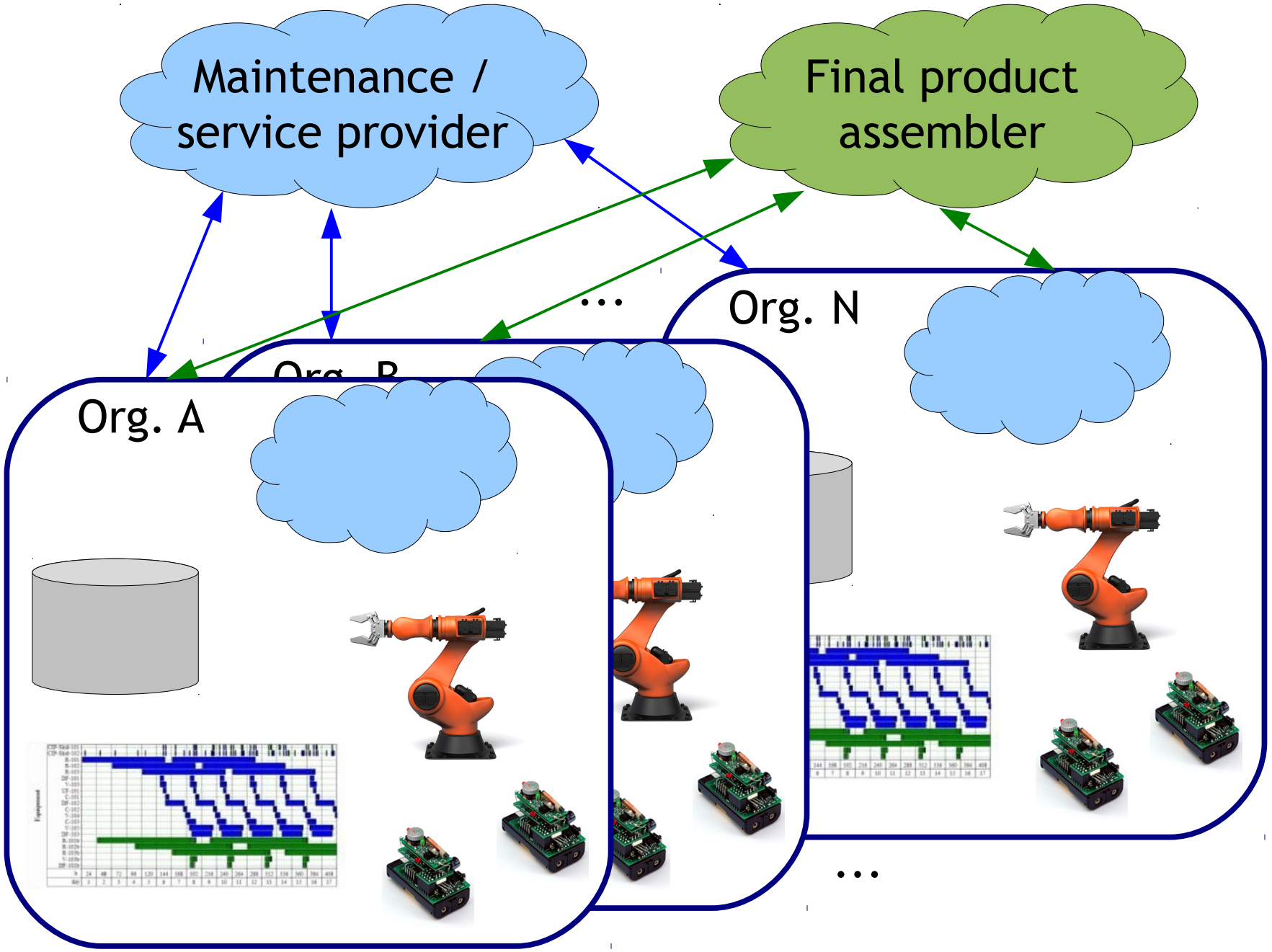
My favorite IoT quote: "That's not the Internet ***of*** Things, that's the Internet ***with*** Things."

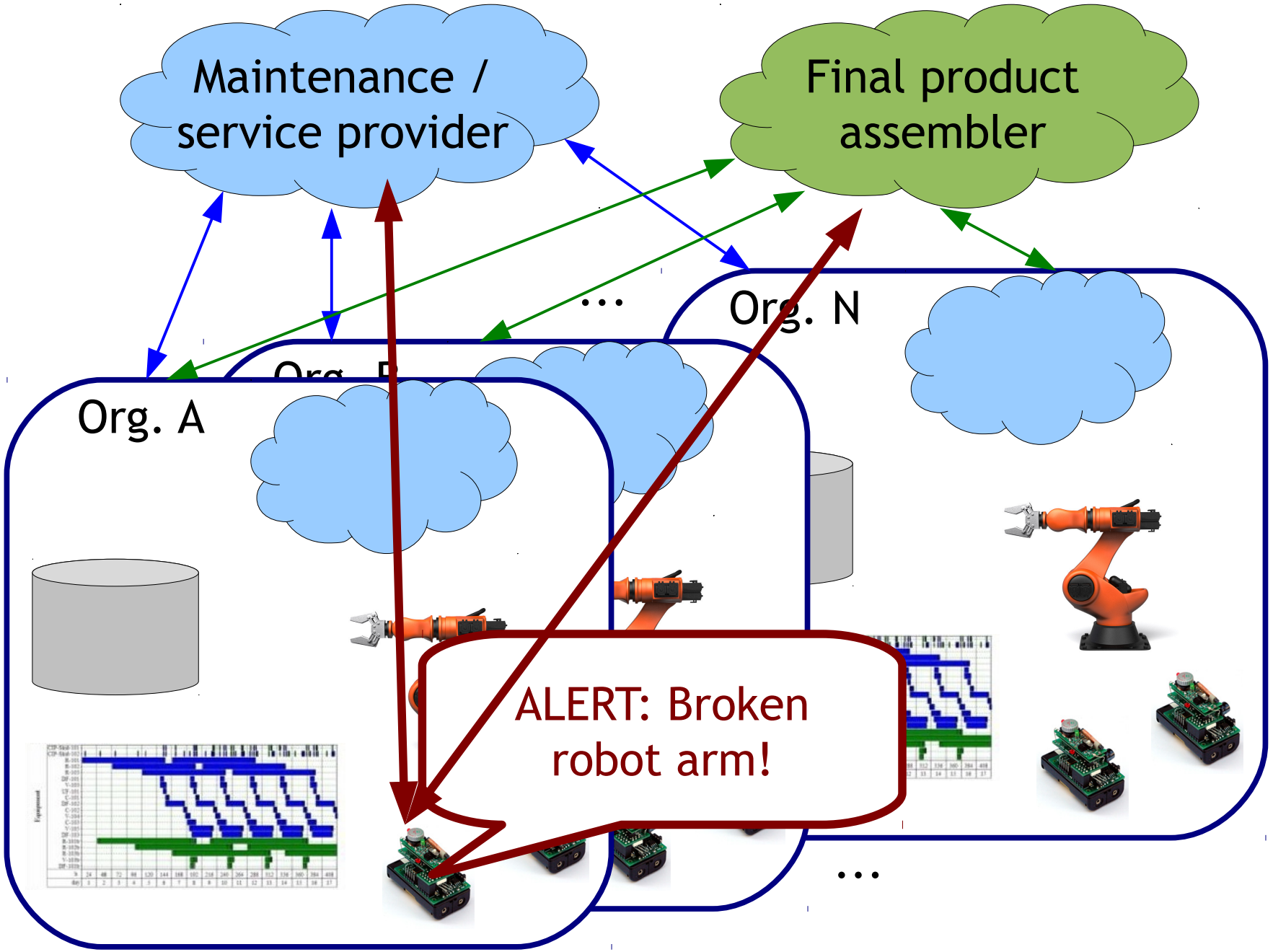
So, the Internet of Things is … ?

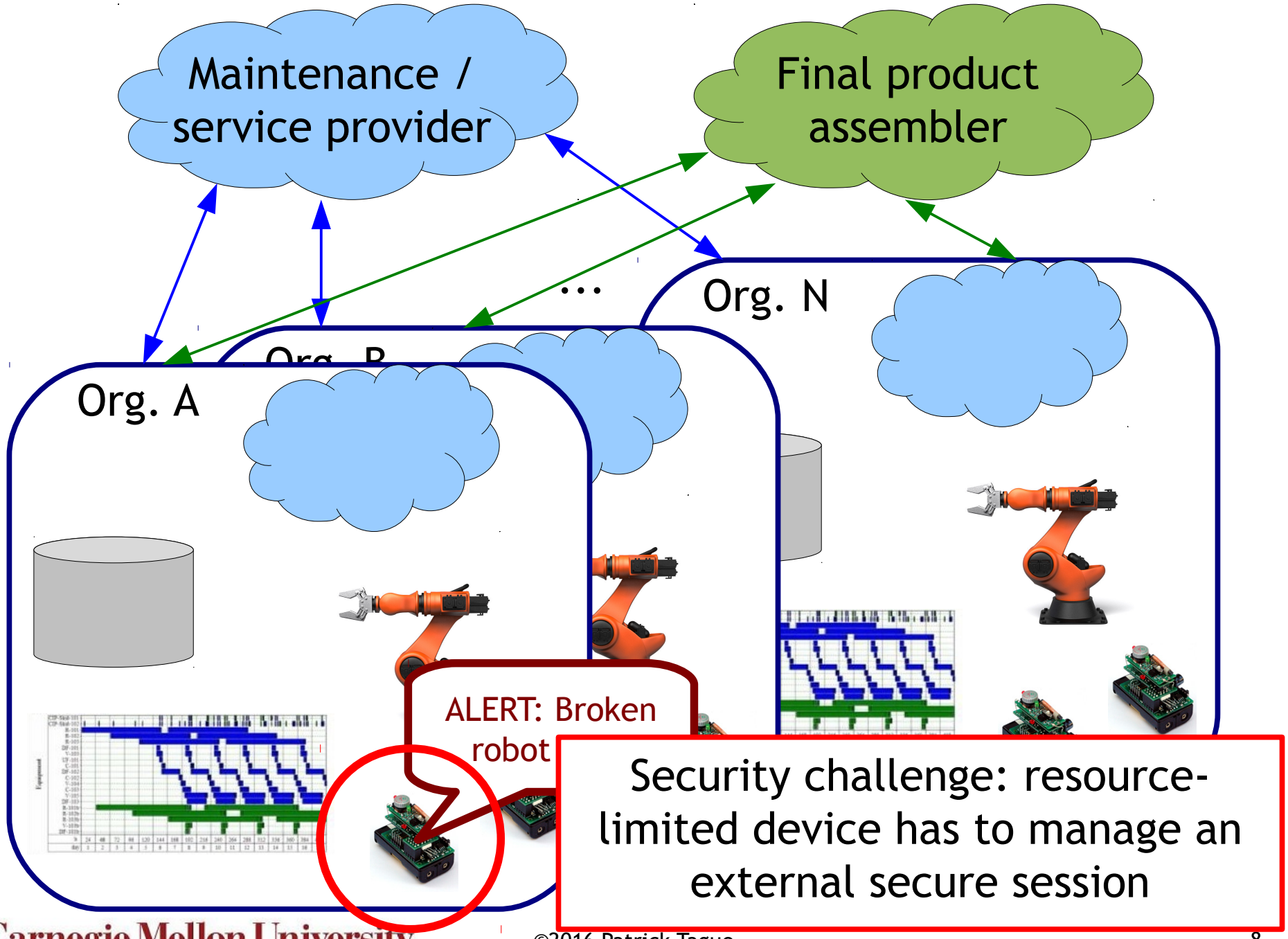
- It's complicated. Everyone has their own definition.

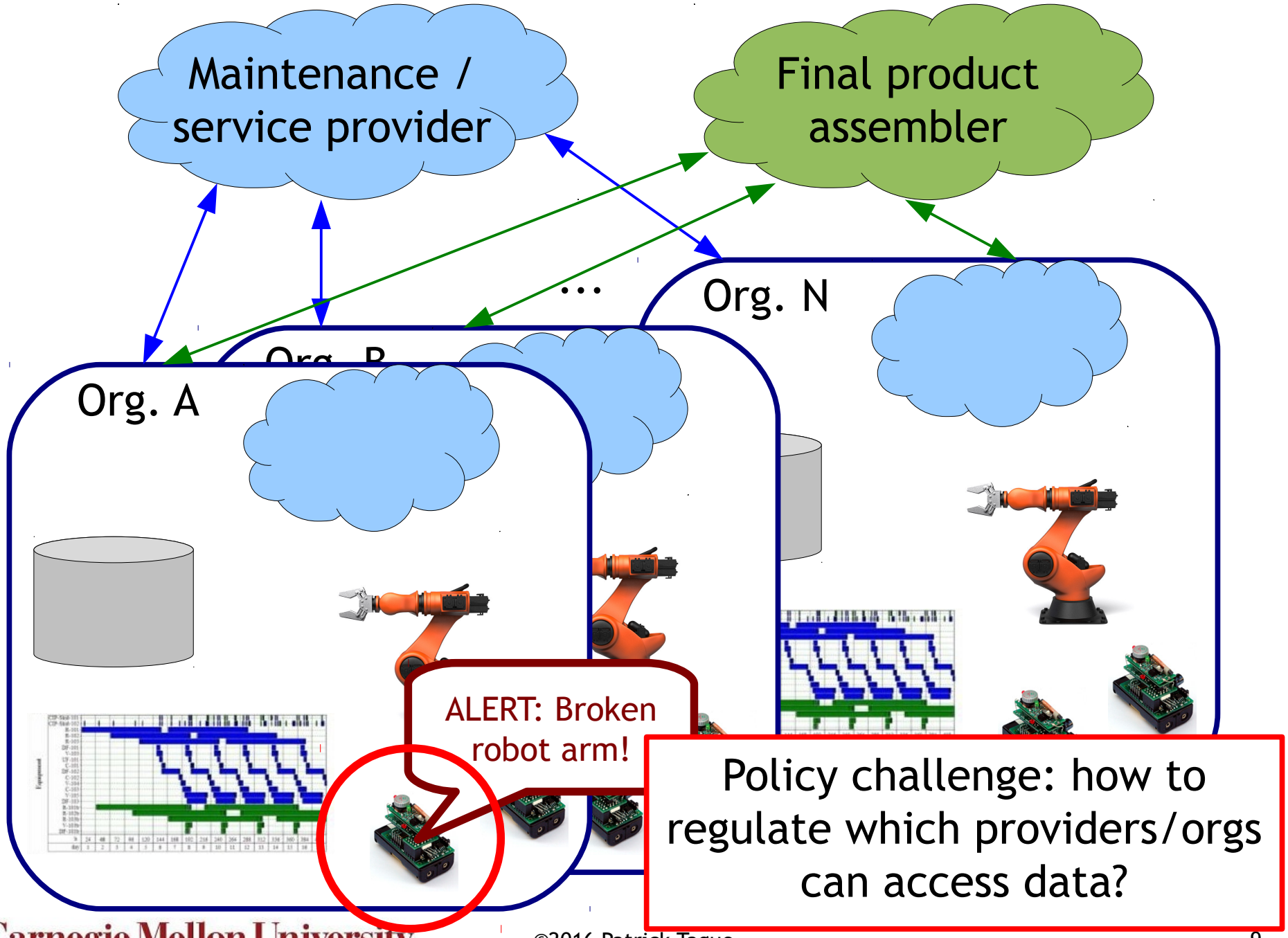
- Most are something to the effect of:
  - Allowing embedded things to collaborate to provide some sort of service to users, apps, or other things
  - Apps can get data from some things, process the data using other things, make decisions using other things, and affect the real world using other things
  - Many of these things are wireless

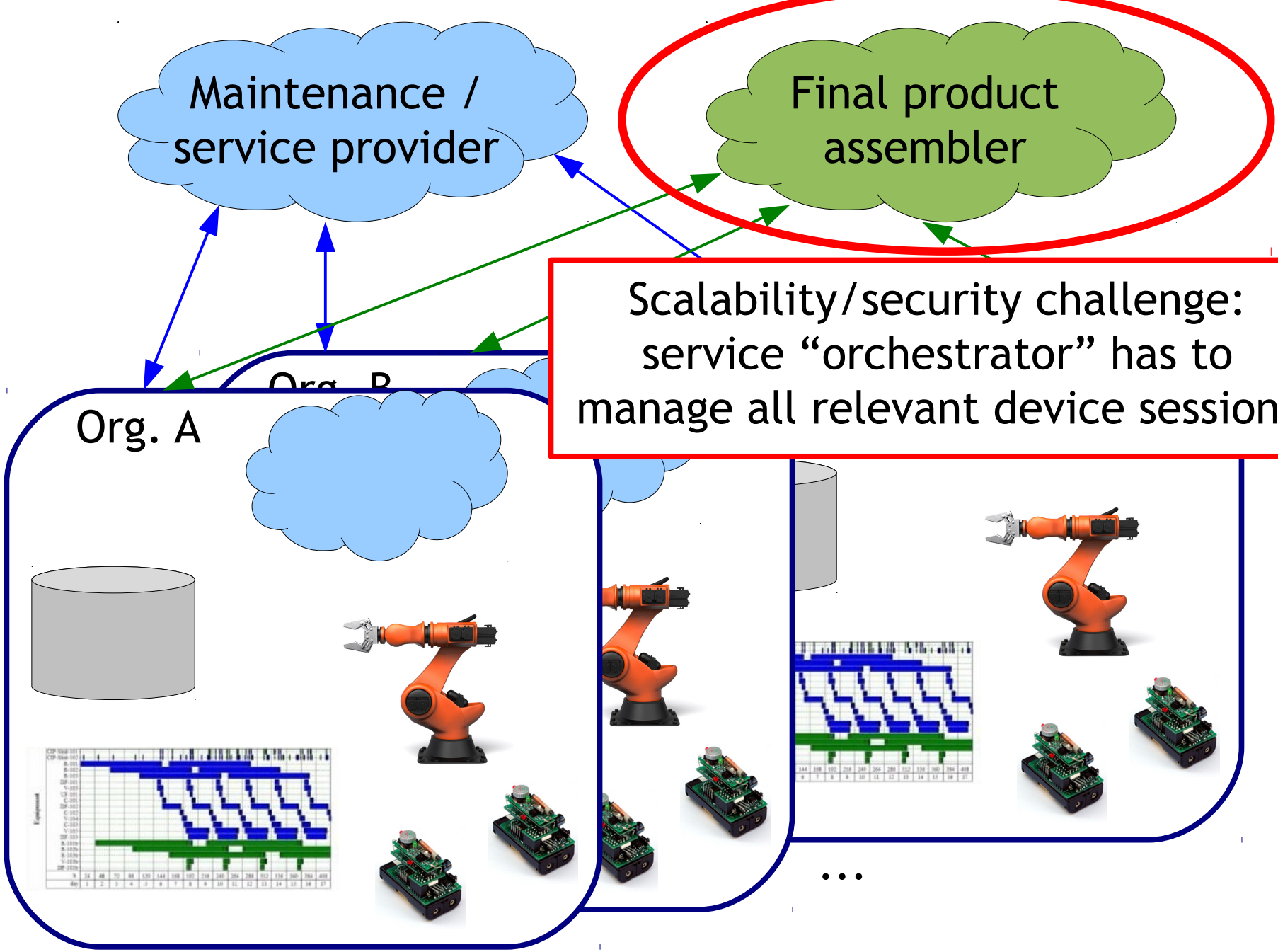
Example 1:
Industrial IoT



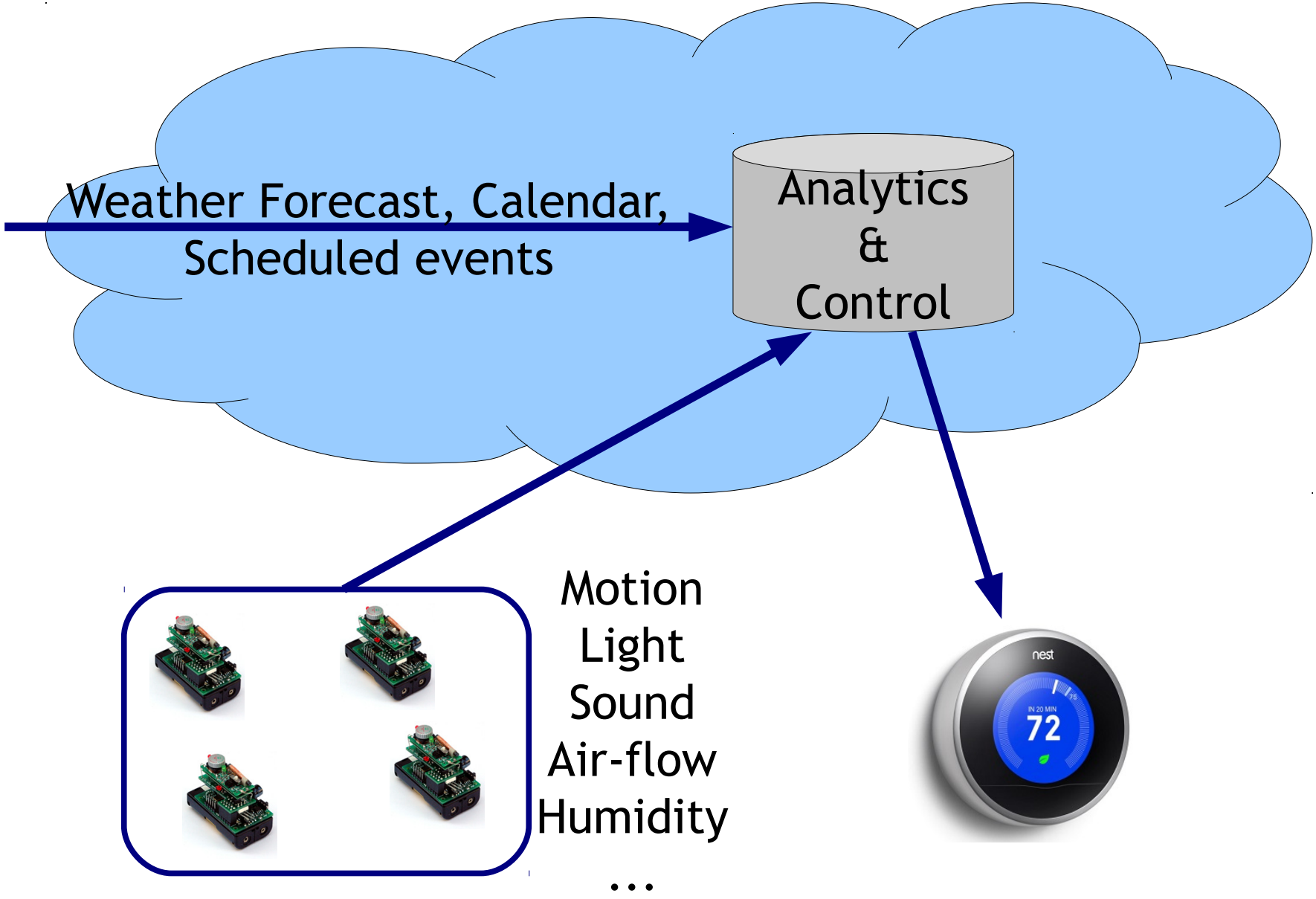


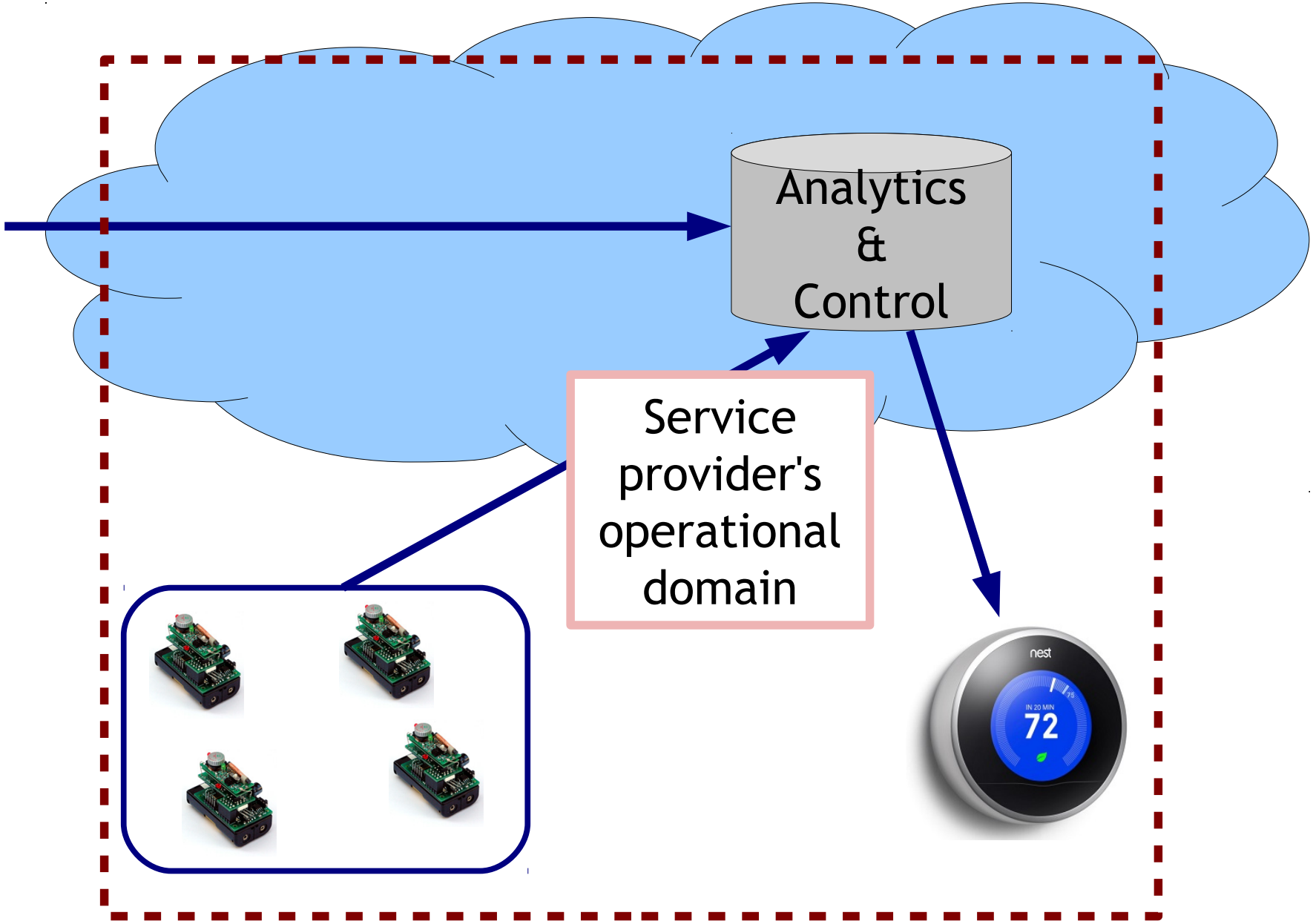


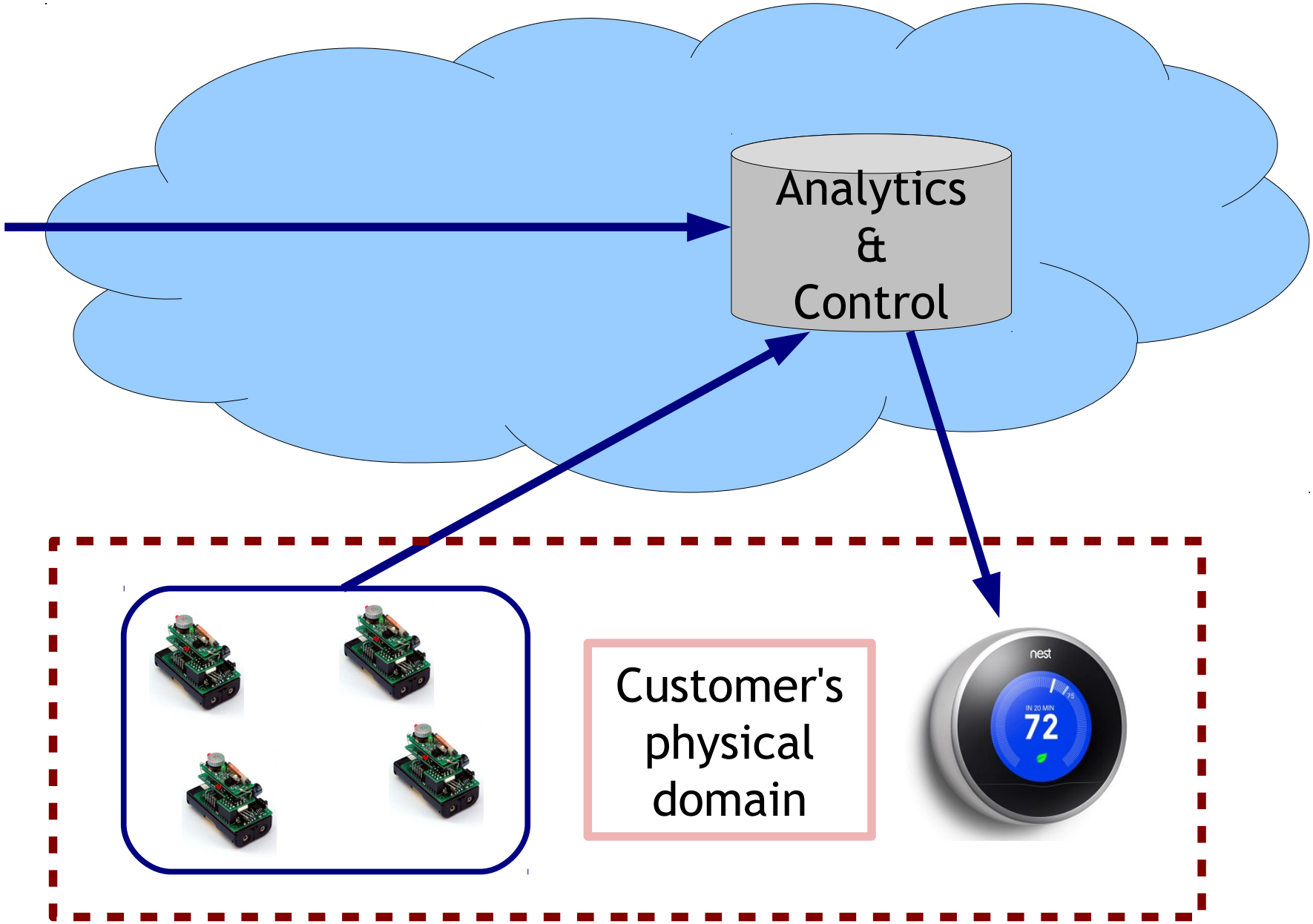


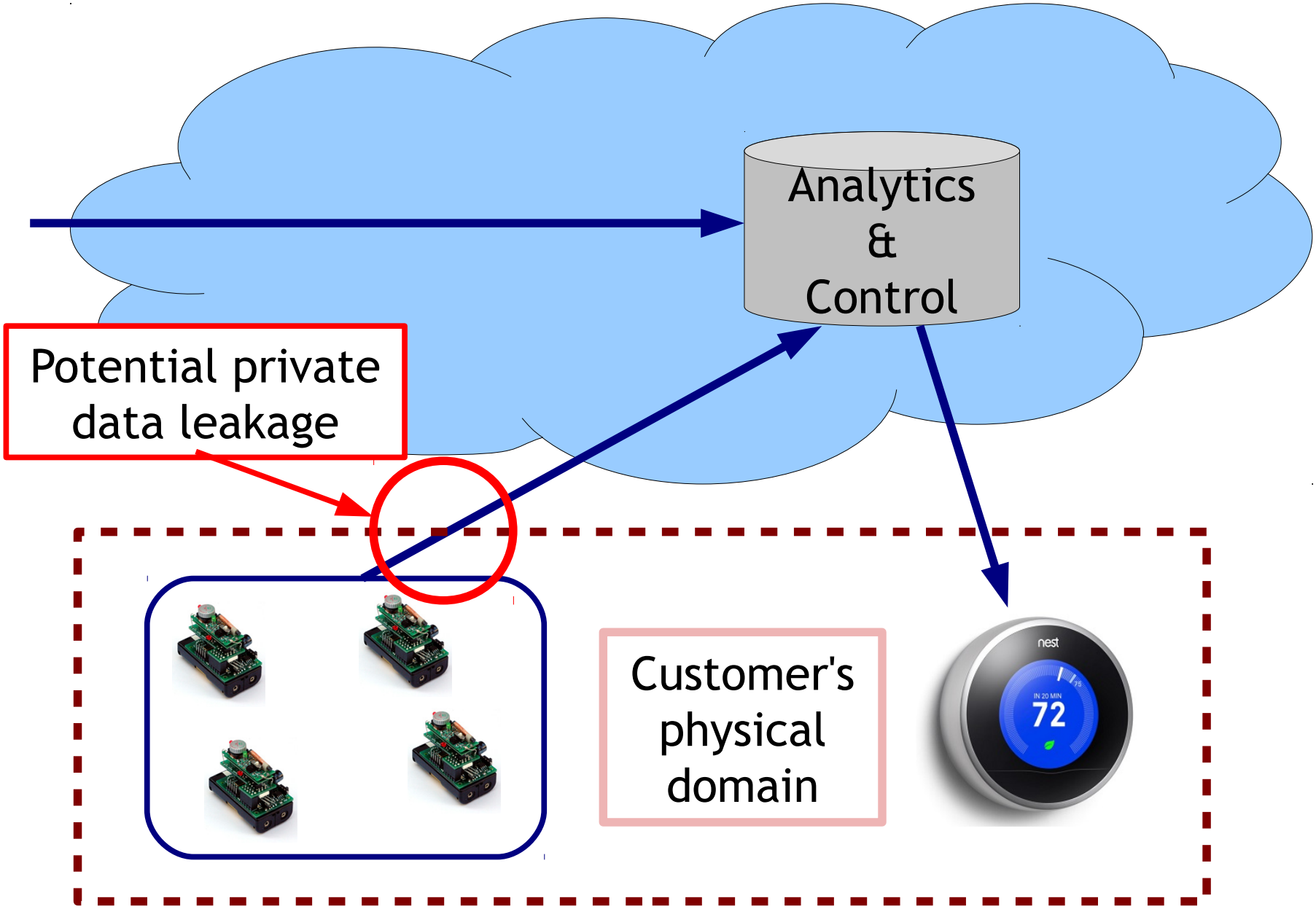


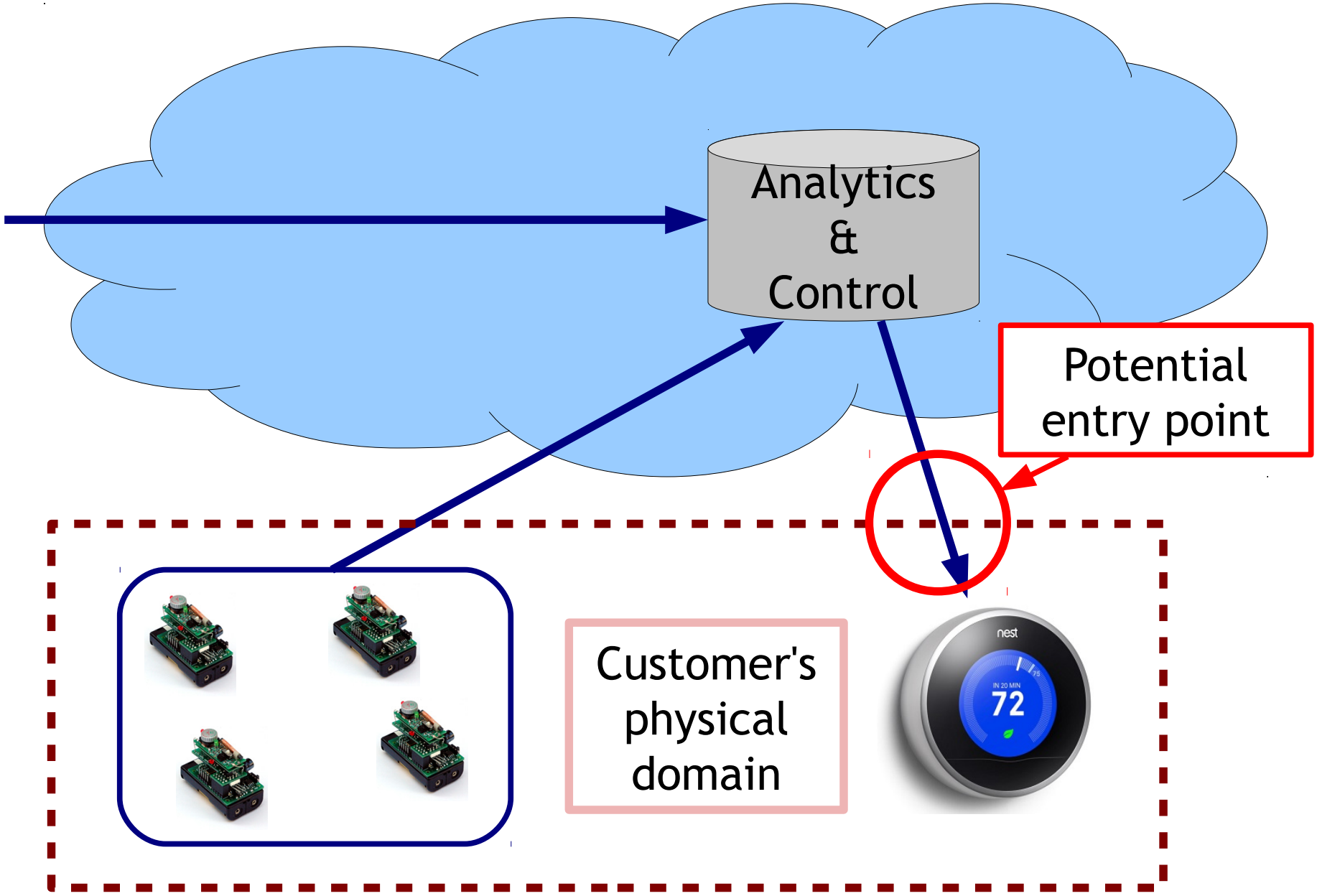
Example 2:
Residential IoT



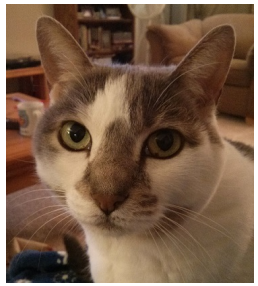




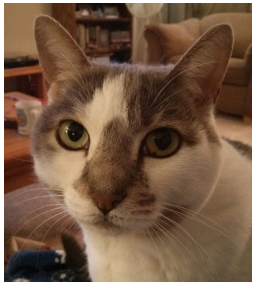


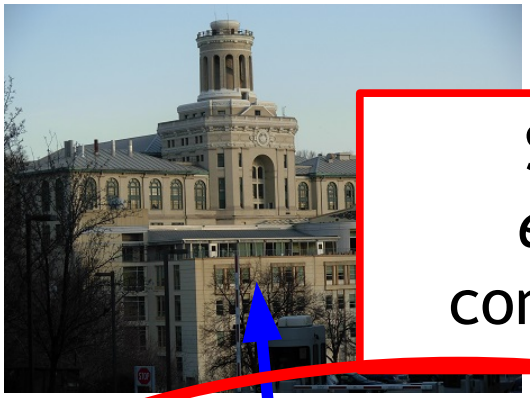


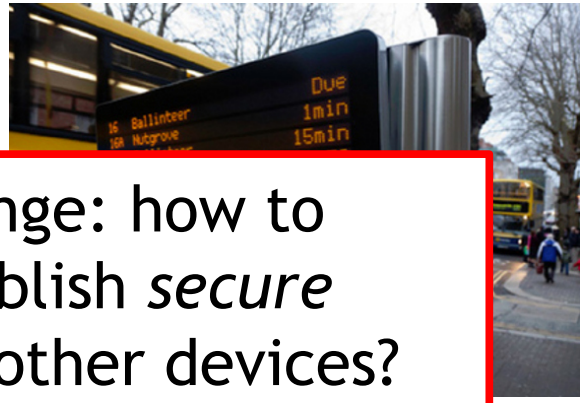
Example 3:
Urban/Civil IoT



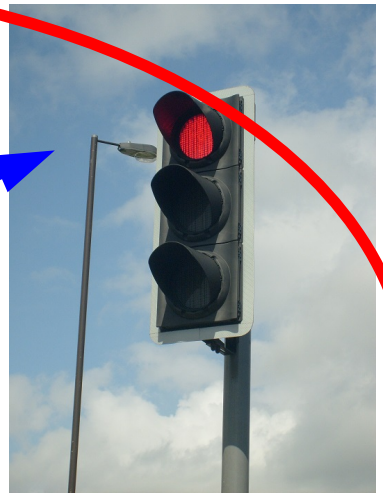
Security challenge: how do devices discover each other and ***verify*** who they discovered?

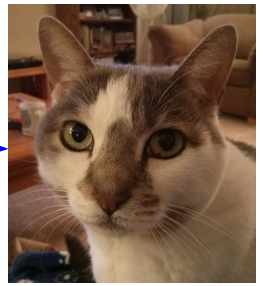


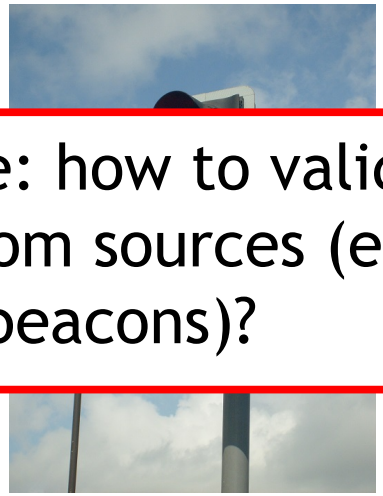




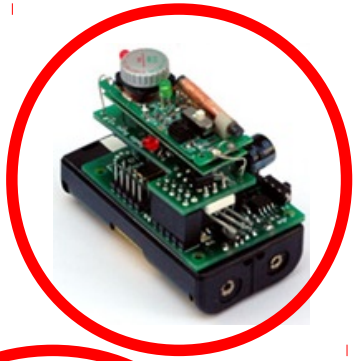
Security challenge: how to *efficiently* establish *secure* connections with other devices?

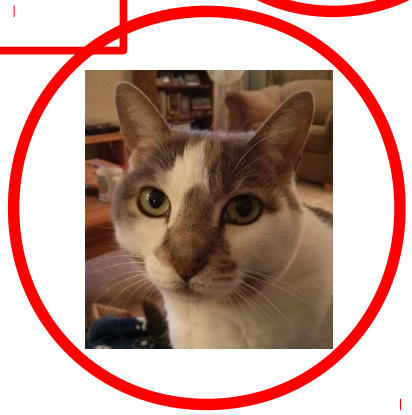






Security challenge: how to validate measurements from sources (e.g., sensors, beacons)?





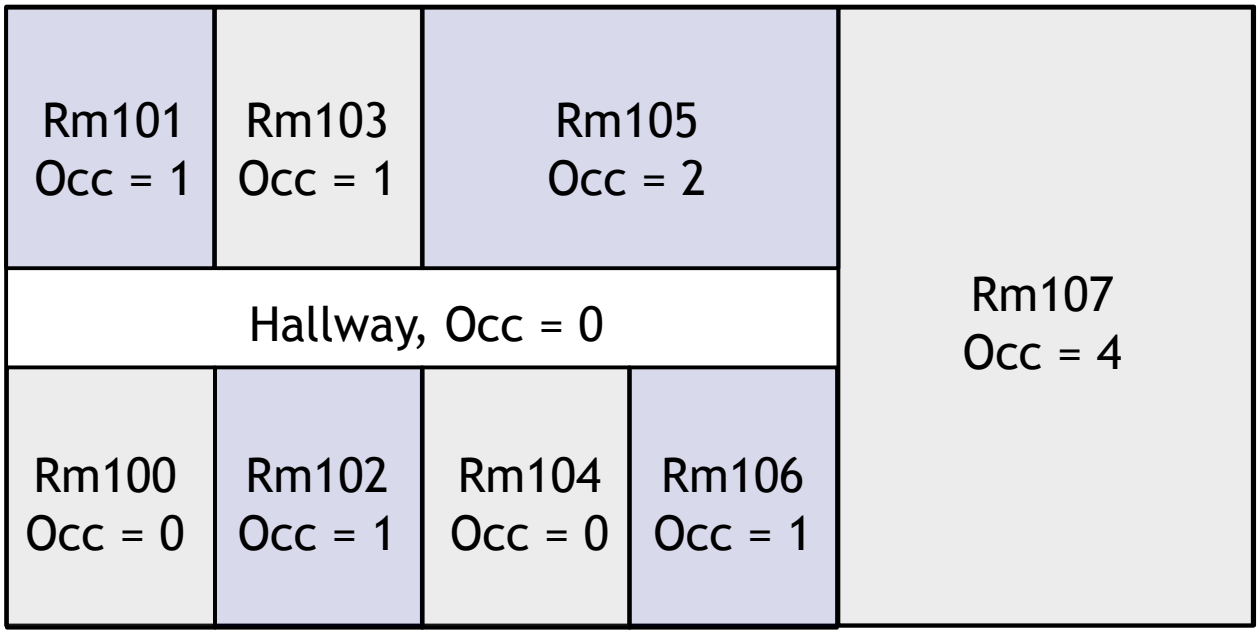
Data-Centric Issues

- Who owns the data?
  - Also, who determines who owns the sensor data?
- How to track where data is created, transported, analyzed, stored, used as input, etc.?
- What data is needed?
  - Does your application need raw sensor data as input, or will something else suffice?
- What information is conveyed in the data?
  - What can your application learn from my data?

When is the information more than the data?

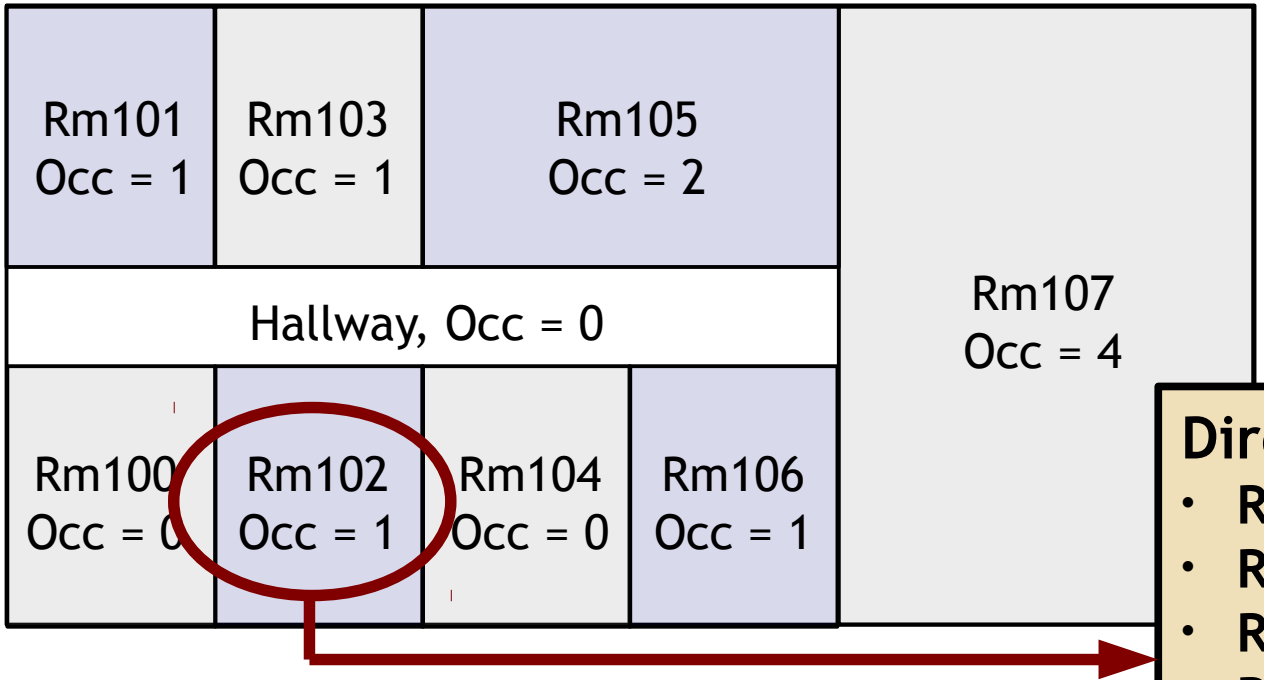
Occupancy

- Occupancy = #people in a room
  - A sensor aggregate that is very valuable for *green* HVAC



It's tempting to say that occupancy is privacy-preserving (in fact, many people have said it)

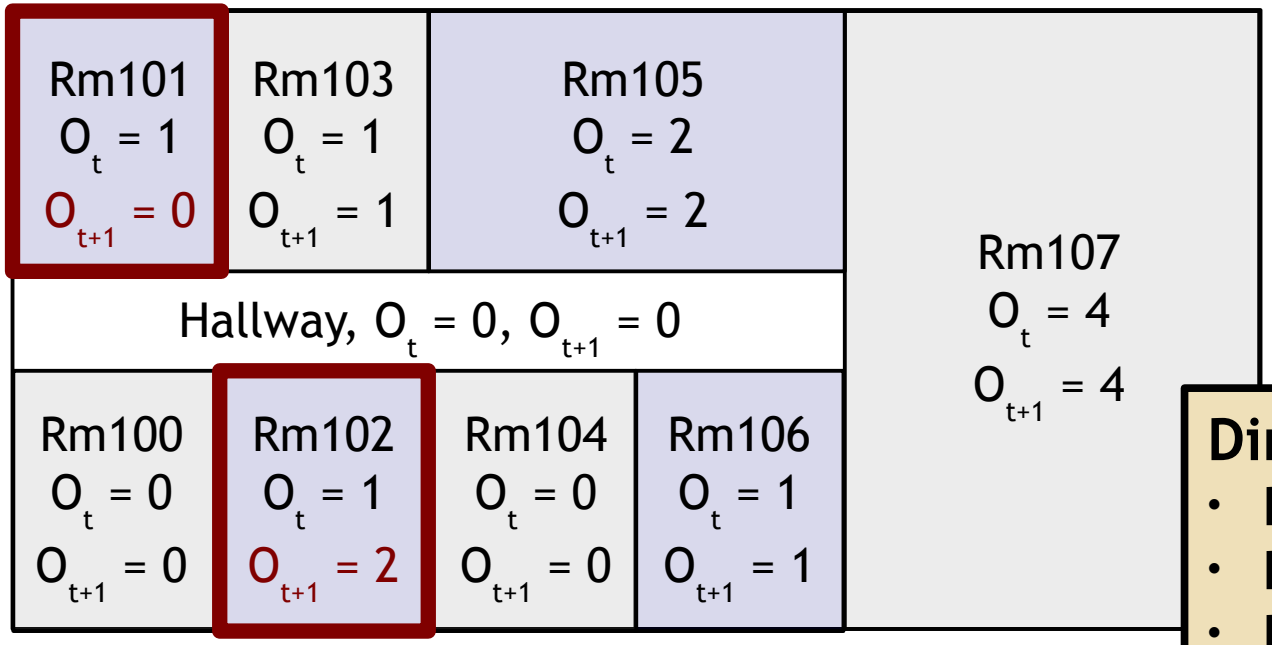
Occupancy + Context



Directory:

- **Rm100**: Aaron's office
- **Rm101**: Beth's office
- **Rm102**: Carlos's office
- **Rm103**: Dennis's office
- **Rm104**: Evelyn's office
- **Rm105**: Shared lab
- **Rm106**: Kitchen
- **Rm107**: Boardroom

Dynamic Occupancy



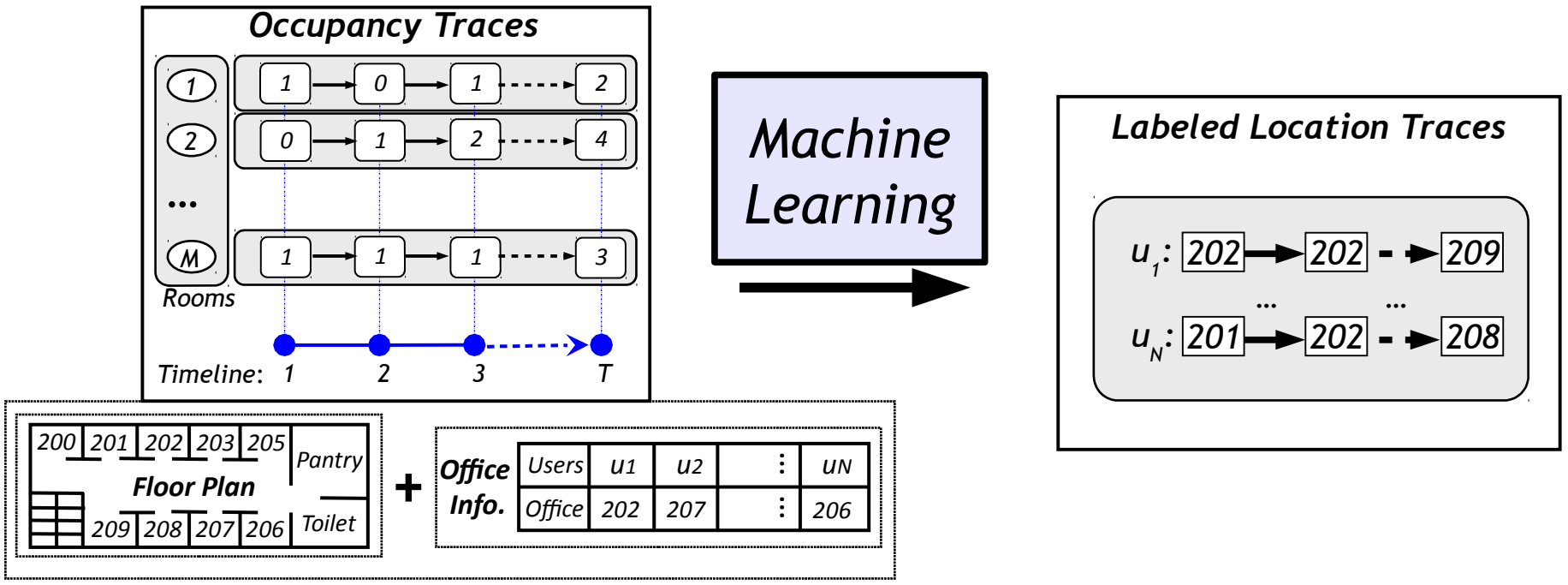
Directory:

- **Rm100**: Aaron's office
- **Rm101**: Beth's office
- **Rm102**: Carlos's office
- **Rm103**: Dennis's office
- **Rm104**: Evelyn's office
- **Rm105**: Shared lab
- **Rm106**: Kitchen
- **Rm107**: Boardroom

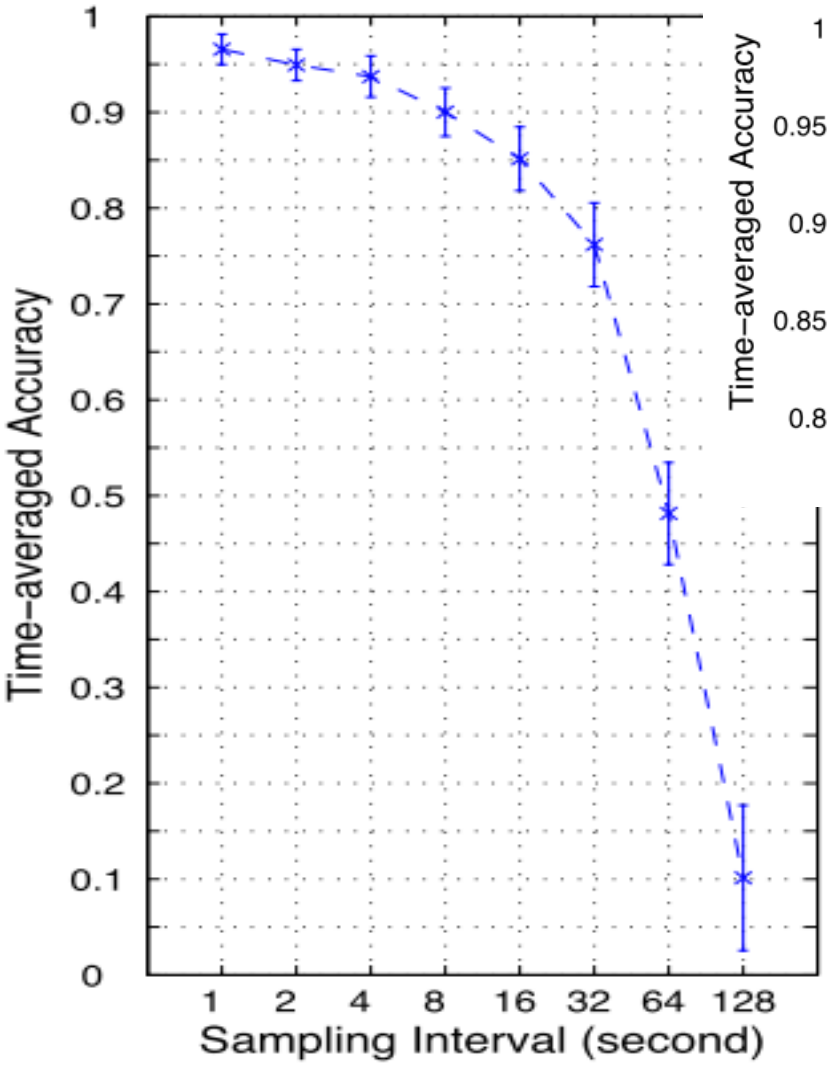
Occupancy ==> Tracking

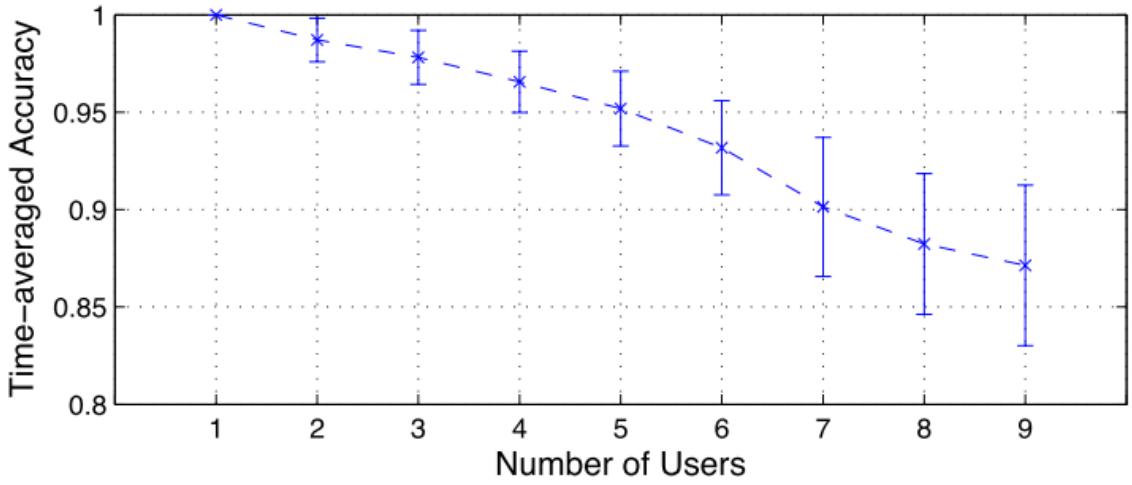
Sufficiently fine-grained occupancy data permits **location trace reconstruction** of building users

Context information permits **labeling** of location traces with **user identity**



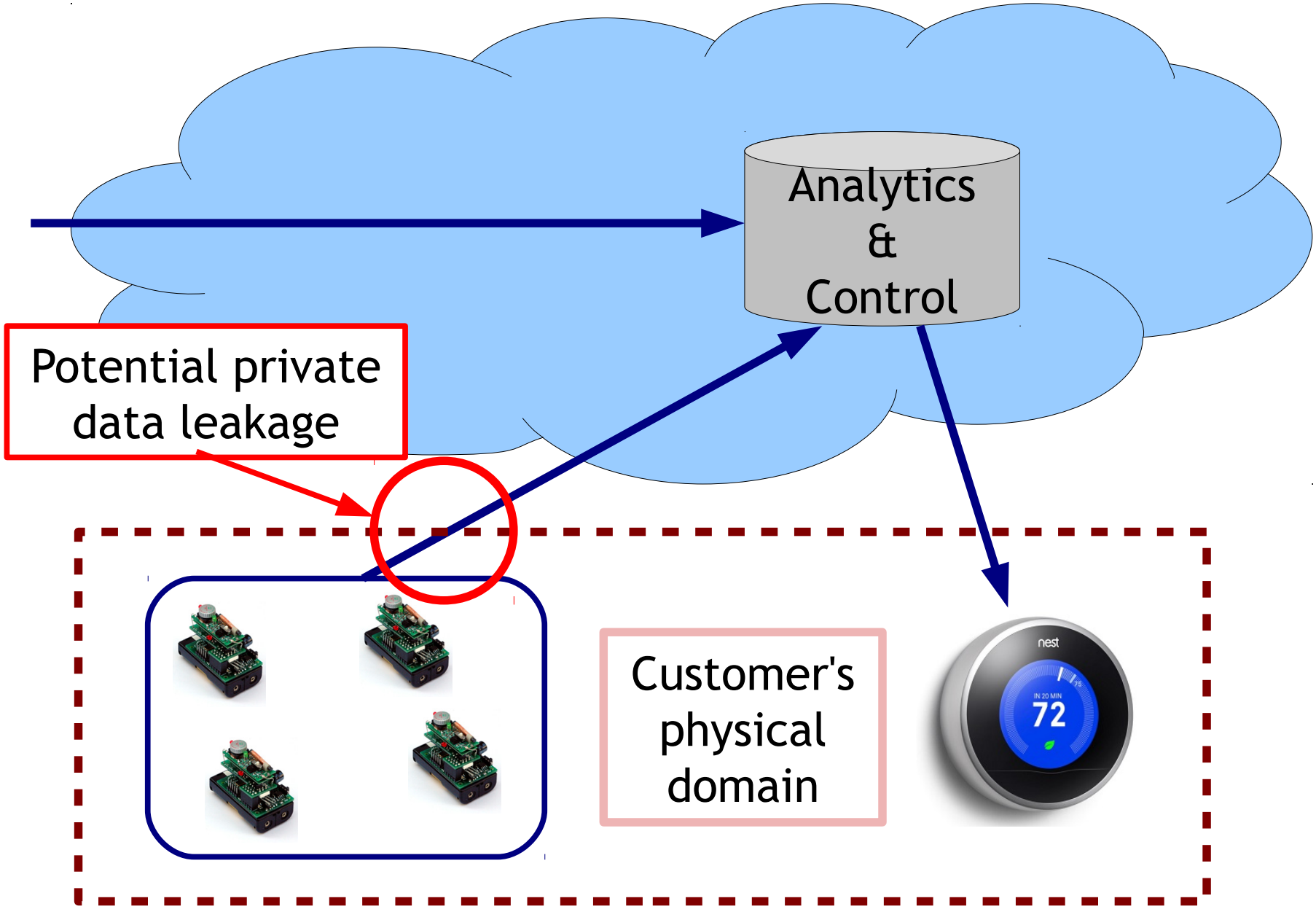
Accuracy ==> Privacy Risk

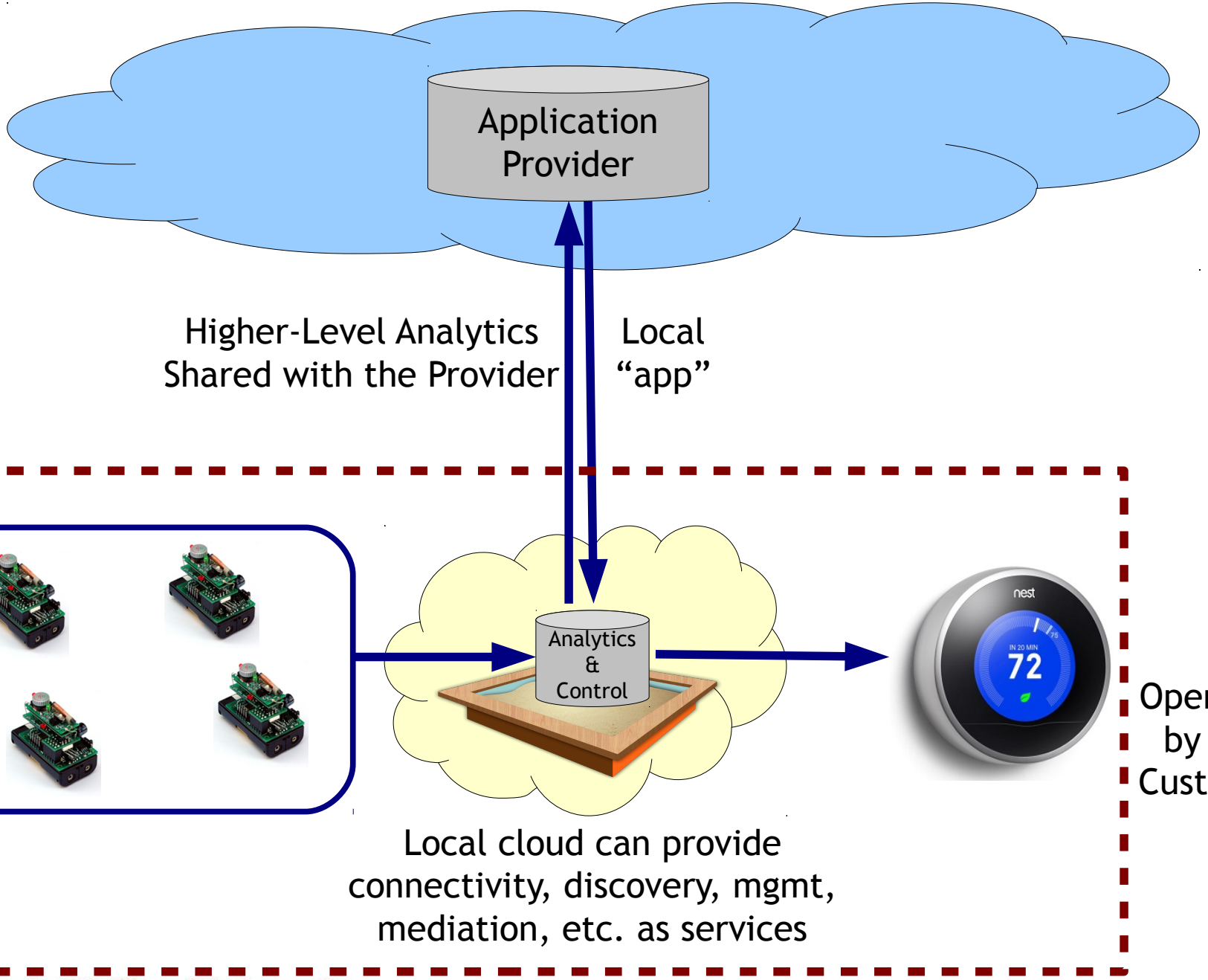




Augsburg benchmark dataset w/ synthetic data; Estimation using FHMM + modified Viterbi algorithm

How can we address these issues?

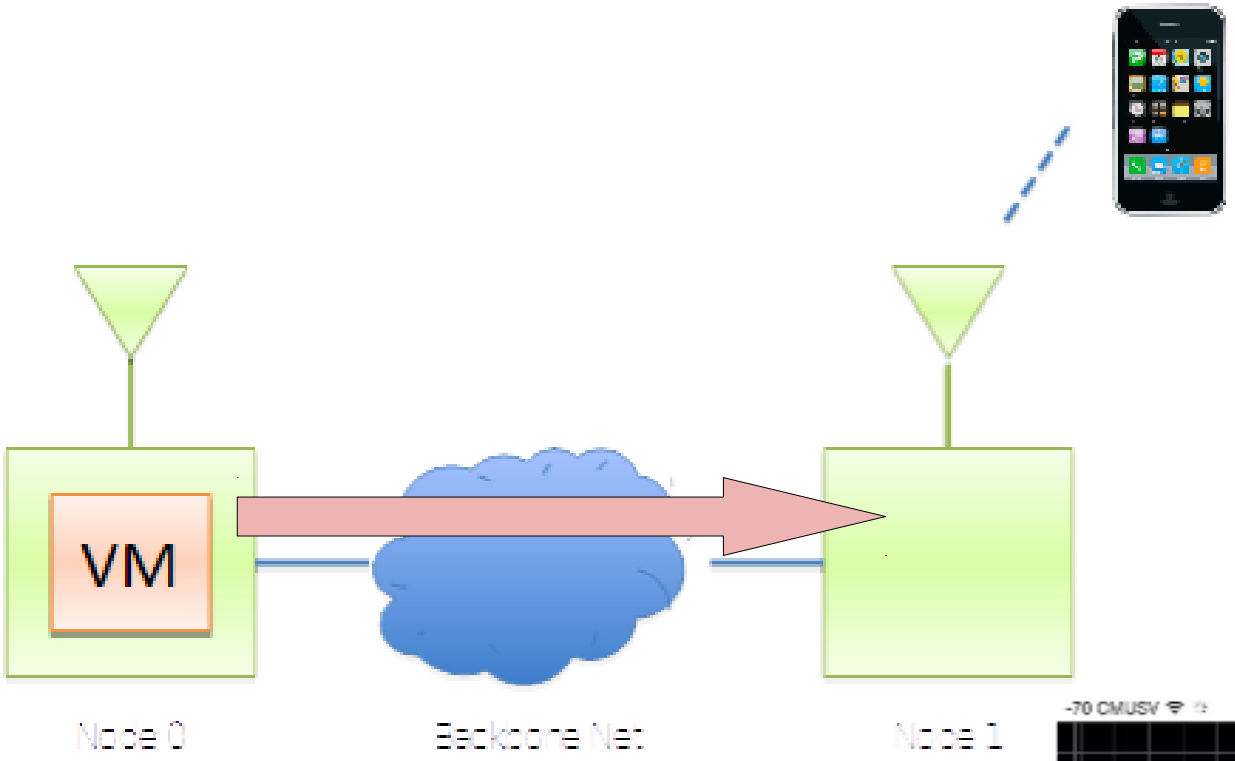


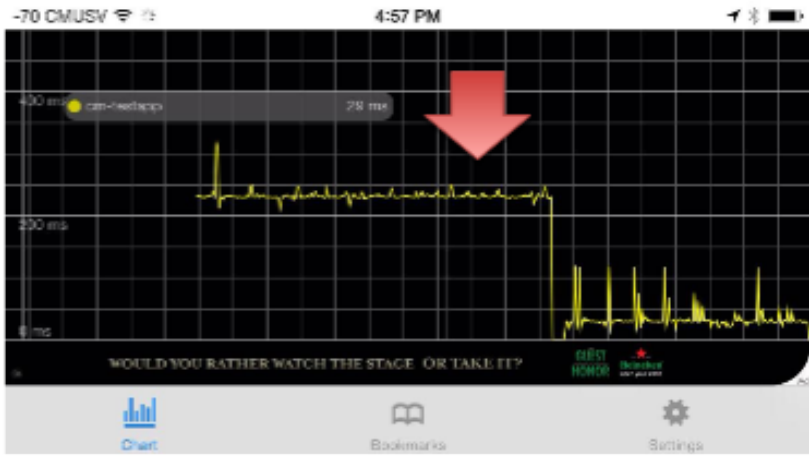


A Few Considerations

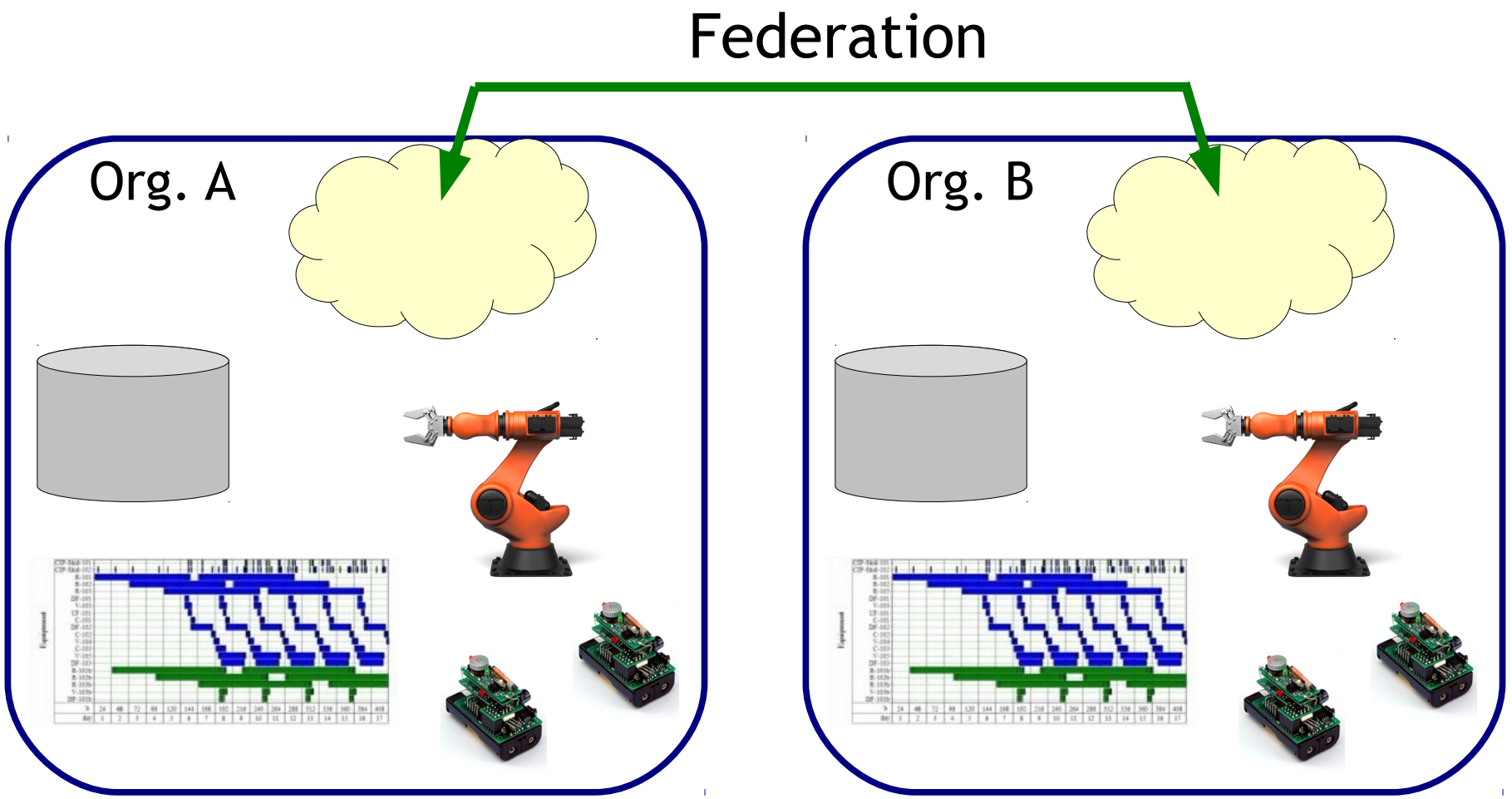
- Local cloud resources can use trustworthy computing principles to securely house 3rd-party software (just like a mobile phone)
- Mediating gateway can actively control information flow between internal devices and third-party resources
- Active migration within the local domain can help with (near-)real-time CPS requirements

Migration

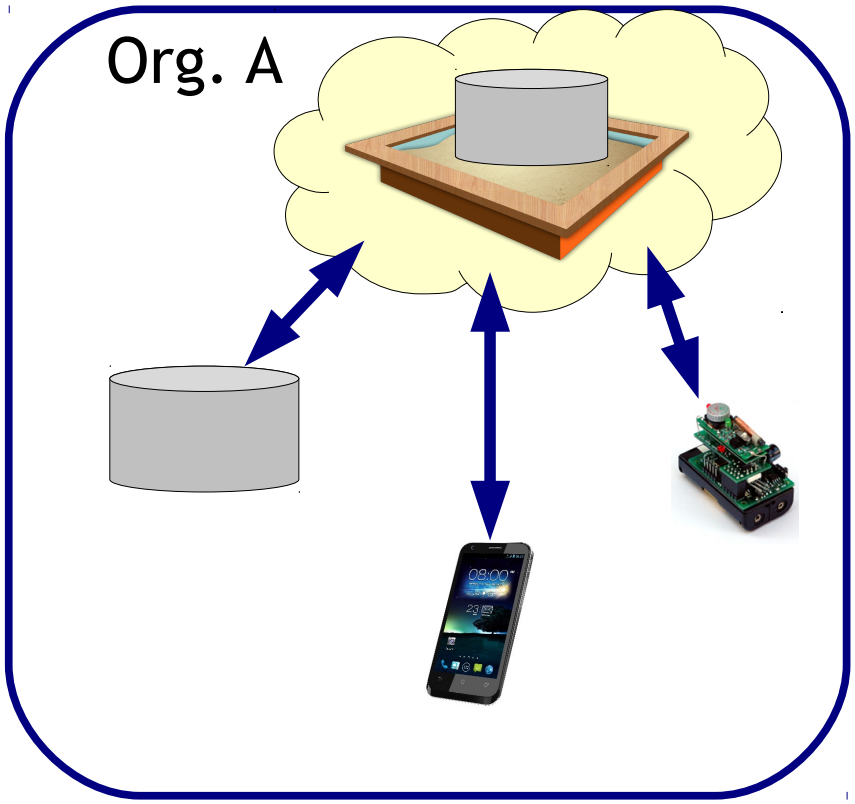




How could two orgs collaborate in a constructive, efficient, privacy-preserving, … manner?



Generalized IoT Domain Model



Intra-domain: everything is managed locally/privately by the domain controller

Inter-domain: domain controllers initiate, mediate, and manage interactions

Take-Away Points

- IoT ≠ Internet (or WoT ≠ Web)
- Domain federation/mediation model allows for finer-grained control of collaboration, sharing, etc. common to IoT applications
- Domain model comes with its own challenges, so still a lot of work to be done

Apr 19:
Telecom Security & Privacy