Security beyond COMSEC

Assume Crypto

- As we've seen this morning, the crypto part is easy!
- So where's the hard part?

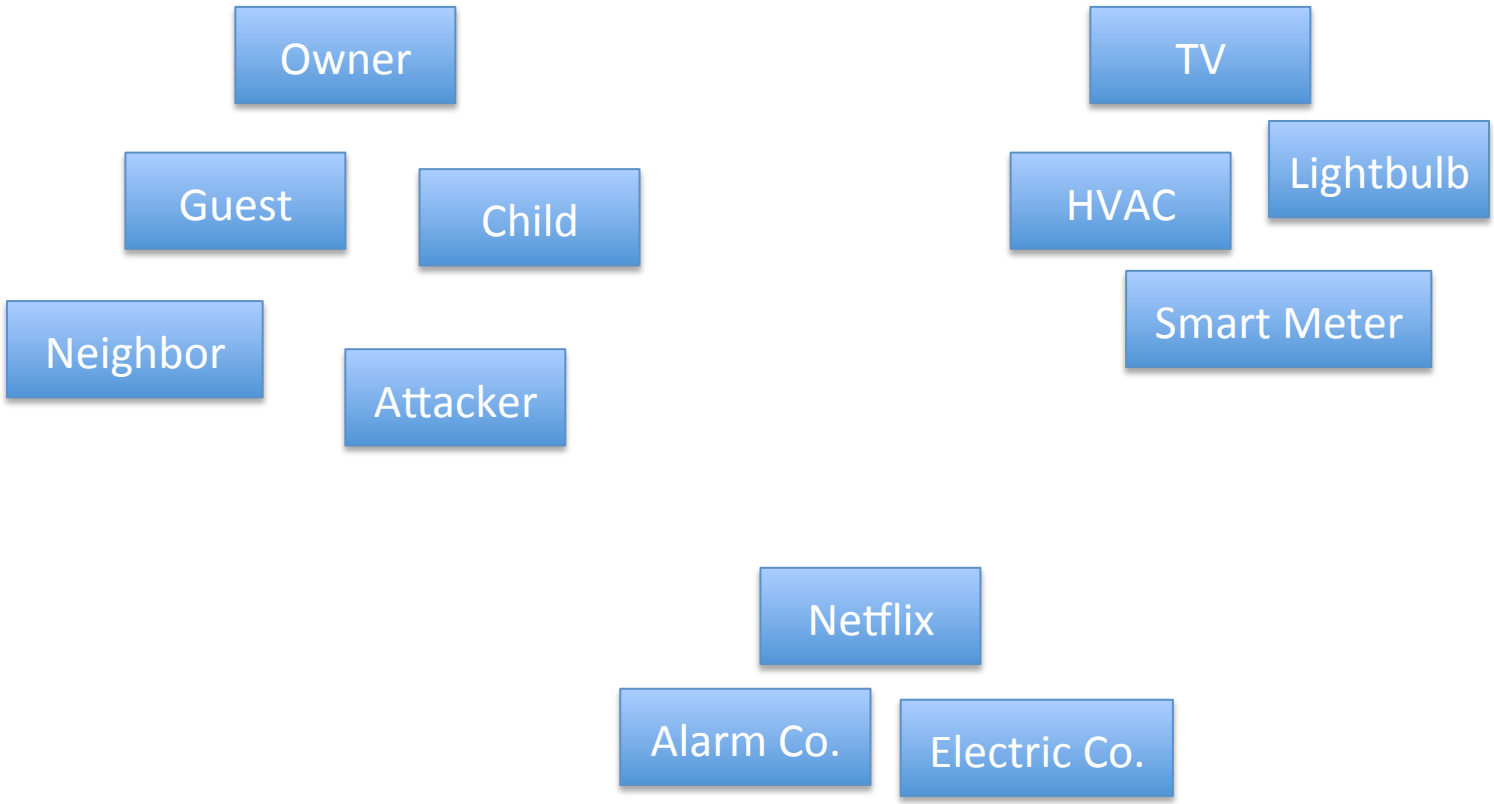
Why are we doing this in the first place?

- We do crypto because we want to control who can do what with data and services
  - Only devices with password can use the network
  - Only a server with the right credentials can act as my bank's web site

Relationships

- Who are the cryptographic entities involved in a system of smart objects? How do they map to physical things?
- How do authorizations get negotiated and enforced?
  - Is “imprinting” all we need?

Principals in the home

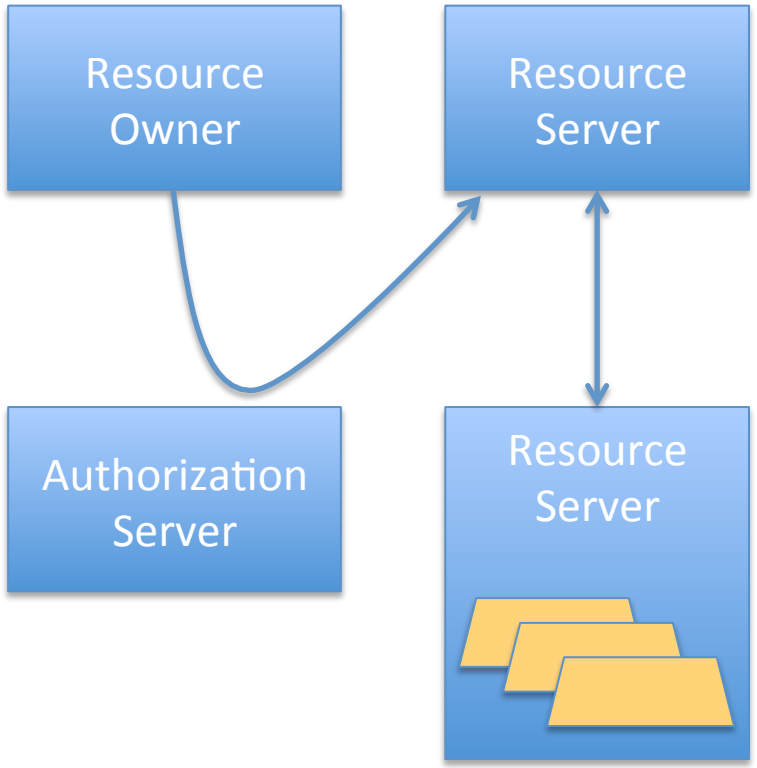


Since time immemorial

- Simple mappings of principals to things
  - User = credentials (password)
  - Web service = certificate
- Simple authorization policies
  - "Only proceed with connection if certificate matches domain in URL"

The next generation: OAuth

- Capabilities decoupled from users
- One principal can pass capability to another
- Already used in some "Internet of things"-like applications
  - Giving your TV access to Netflix



Questions

- Where does identity come from?
  - Key hashes, plus barcodes / RFIDs?
  - Needs to be mutual
- How does authorization originate and flow?
  - Who gets to make authorization decisions?
  - Who can delegate authorizations?
  - Where do authorizations get enforced?
- Is any of this general, or all application-specific?