How secure is your smart home?

Correctness and Security for Home Automation

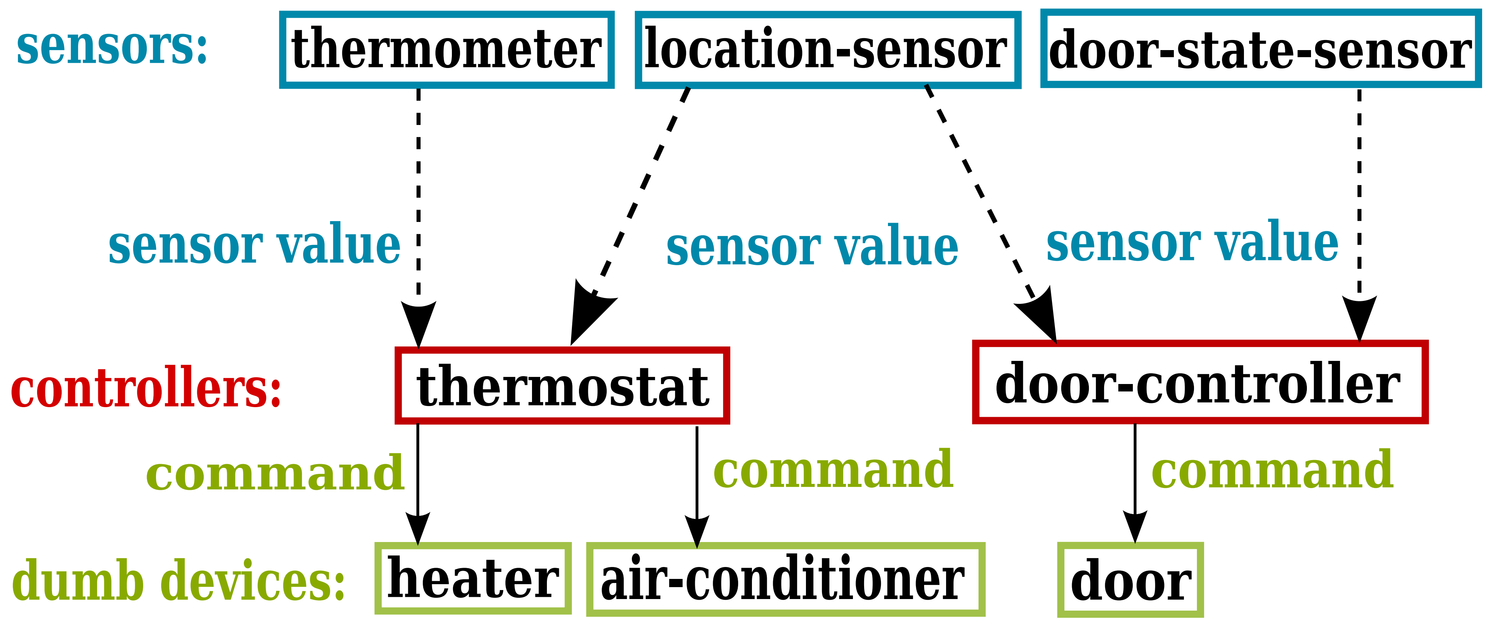
Chandrakana Nandi
Advisor: Michael D. Ernst
University of Washington, Seattle
cnandi@cs.washington.edu

Goal: verify whether interacting smart devices behave correctly

Contributions

- Architecture
- Security policies:
  - dependency policy
  - control policy
  - new item policy

Architecture



Dependency Policy

Controllers should send commands to dumb devices depending on sensor values.

complete specification: controller sends command $\iff$ <sensor_variable=state>$^+$

partial specification: controller sends command $\implies$ <sensor_variable=state>$^+$

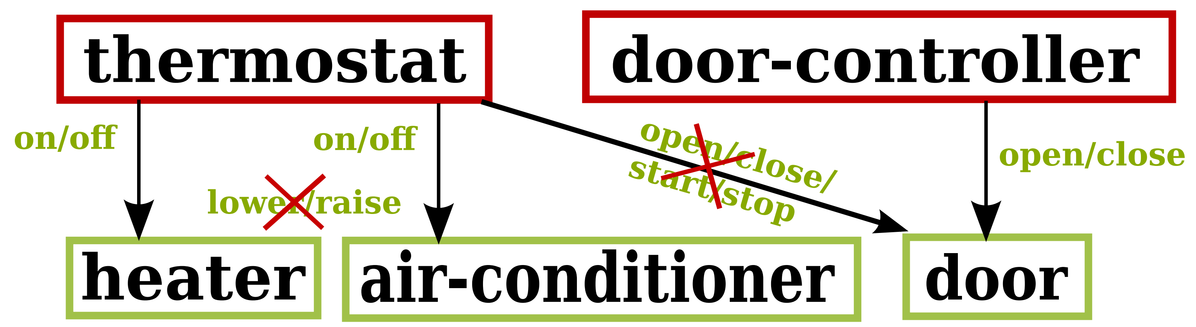
GARAGEDOOR_CONTROLLER sends open_garagedoor $\iff$
$(\neg$ IS_GARAGE_OPEN$)$
$\wedge$ (($\neg$ IS_CAR_INSIDE_GARAGE $\wedge$ CAR_DISTANCE $\leqslant$ "50m" $\wedge$ CAR_SPEED $\neq 0$)
$\vee$ (IS_CAR_INSIDE_GARAGE $\wedge$ IS_CAR_RUNNING))
$\wedge$ (IS_OWNER_INSIDE_CAR)

DISHWASHER_CONTROLLER sends start_dishwasher $\implies$
$(\neg$ IS_DISHWASHER_ON$) \wedge ($IS_DOOR_CLOSED$) \wedge (\neg$ IS_CLEANED$)$
$\wedge (\neg$ IS_EMPTY$)$

New Item Policy

new sensor: no_action
new dumb-device: no_action
new controller: verify_dependency_policy (this)
$\wedge$ verify_control_policy (this)

Control Policy



A controller k maintains a list of commands, $C = \{ c_1, c_2, ..., c_m \}$ and a list of dumb devices, $D = \{ d_1, d_2, ..., d_n \}$. Each $d_i \in D$ maintains a list of actions, $A_{p_i} = \{ a_{i1}, a_{i2}, ..., a_{ip_i} \}$ it can execute.

k should not send:
- right commands to wrong dumb devices
- wrong commands to right dumb devices
- wrong commands to wrong dumb devices

$\forall$ command_dumbdevice sent by k,
$\exists\ c_i \in C \mid$ command_dumbdevice $= c_i$
$\wedge\ \exists\ d_j \in D \mid$ dumbdevice $= d_j$
$\wedge$ command $\in A_{p_j}$

POPL 2016 Student Research Competition, January 2016, St. Petersburg, Florida, USA.