IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery

Wenbo Ding[1] Hongxin Hu[2] Long Cheng[1]

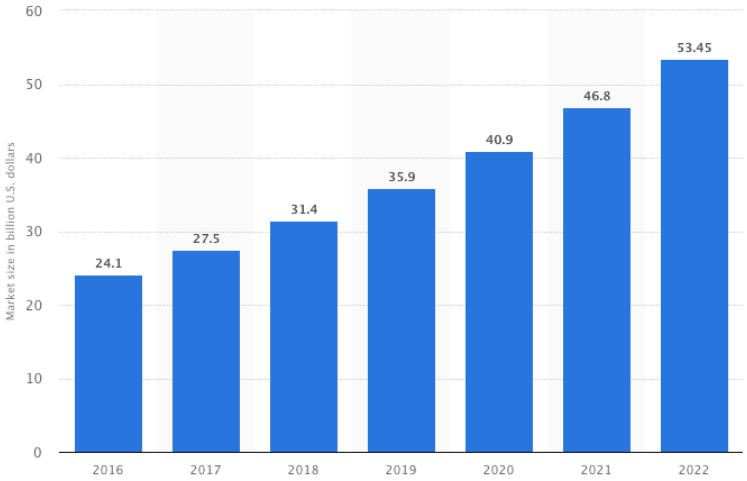
1 CLEMSON UNIVERSITY

2 University at Buffalo

NDSS 2021

Background

- Market size is huge
- Devices are fast-growing
- Provided functions are more complicated



- Smart home platforms

HomeKit

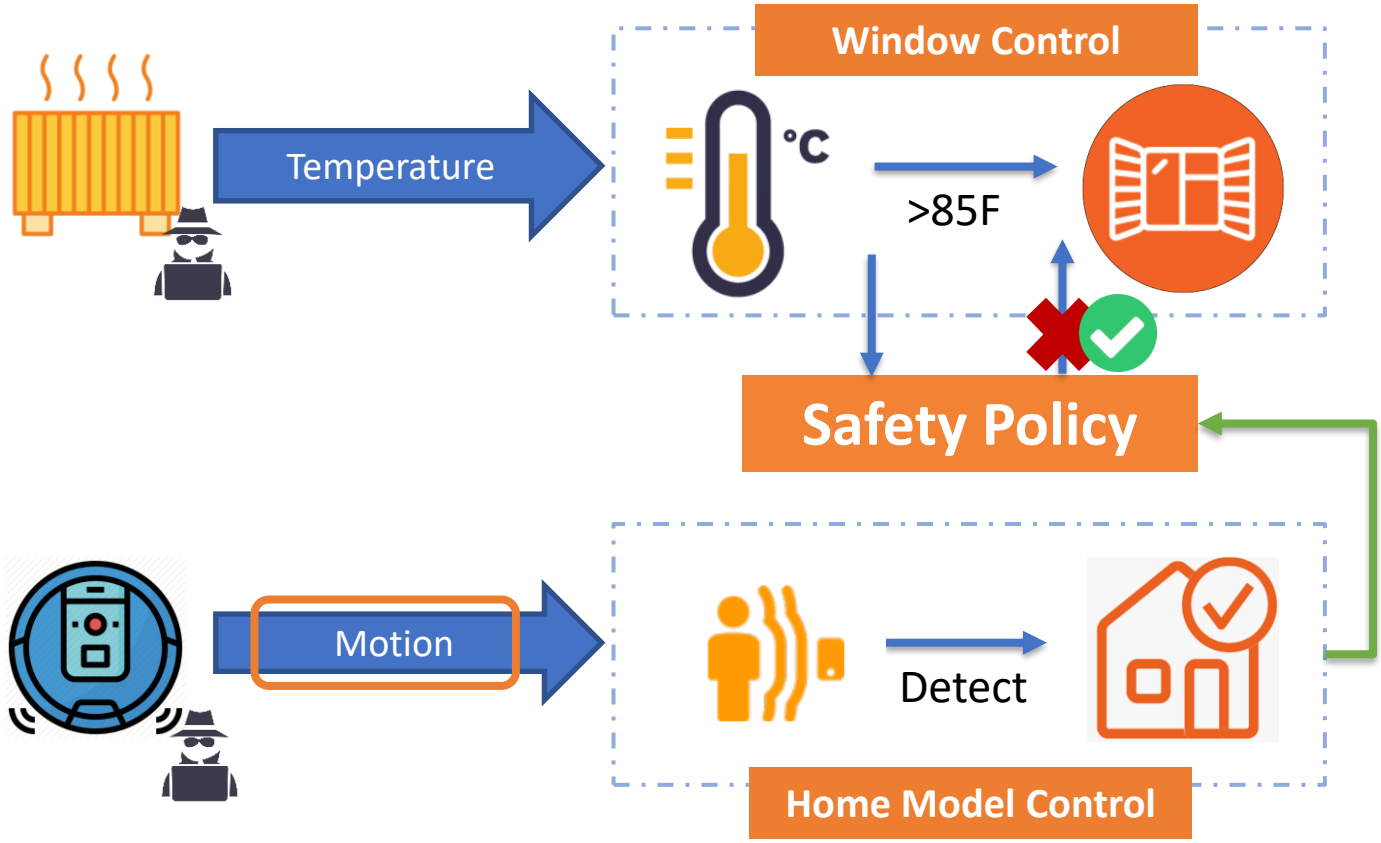
amazon echo

SmartThings™

Physical Interaction

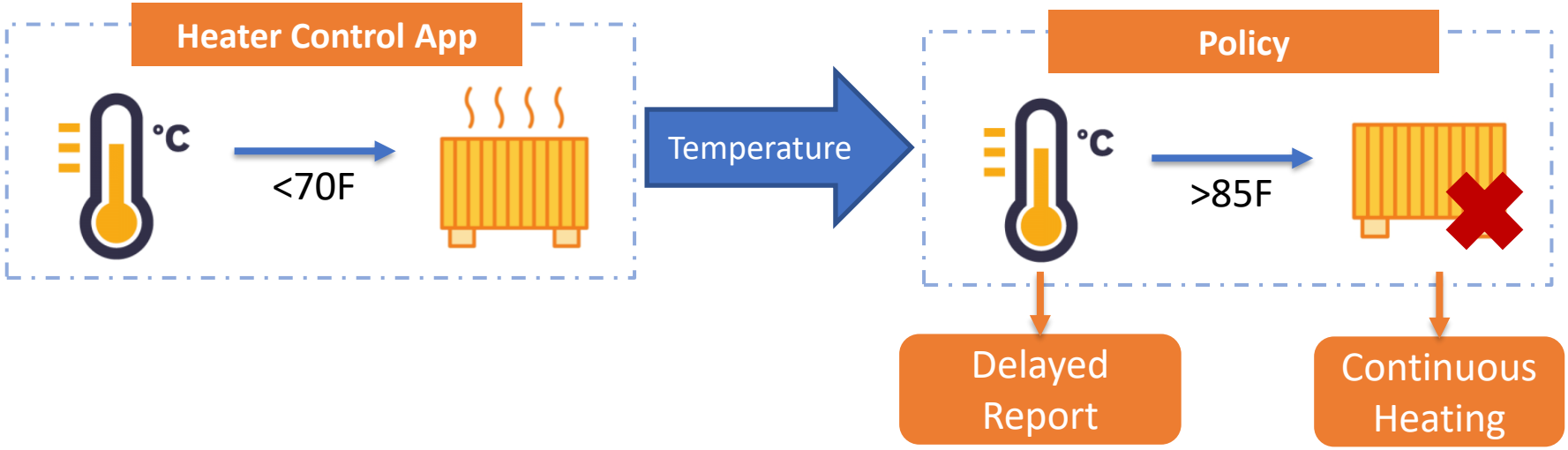
Motivation

- Current policy enforcement systems cannot capture **real** physical interactions between IoT devices.
- Safety/Security Policy
  - "Do not open the window if no one is at home."



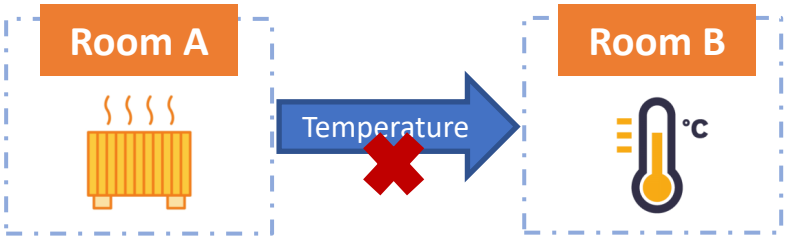
Motivation

- Safety/Security Policy
  - "Turn off the heater when the infant room temperature is above 85F."



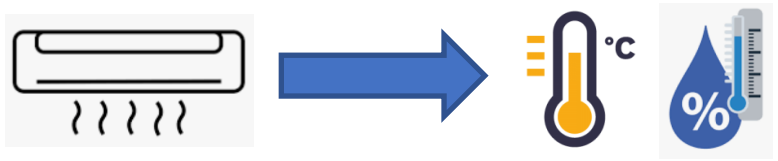
Challenges

- Identifying Real Physical Interactions
  - Spatial Context



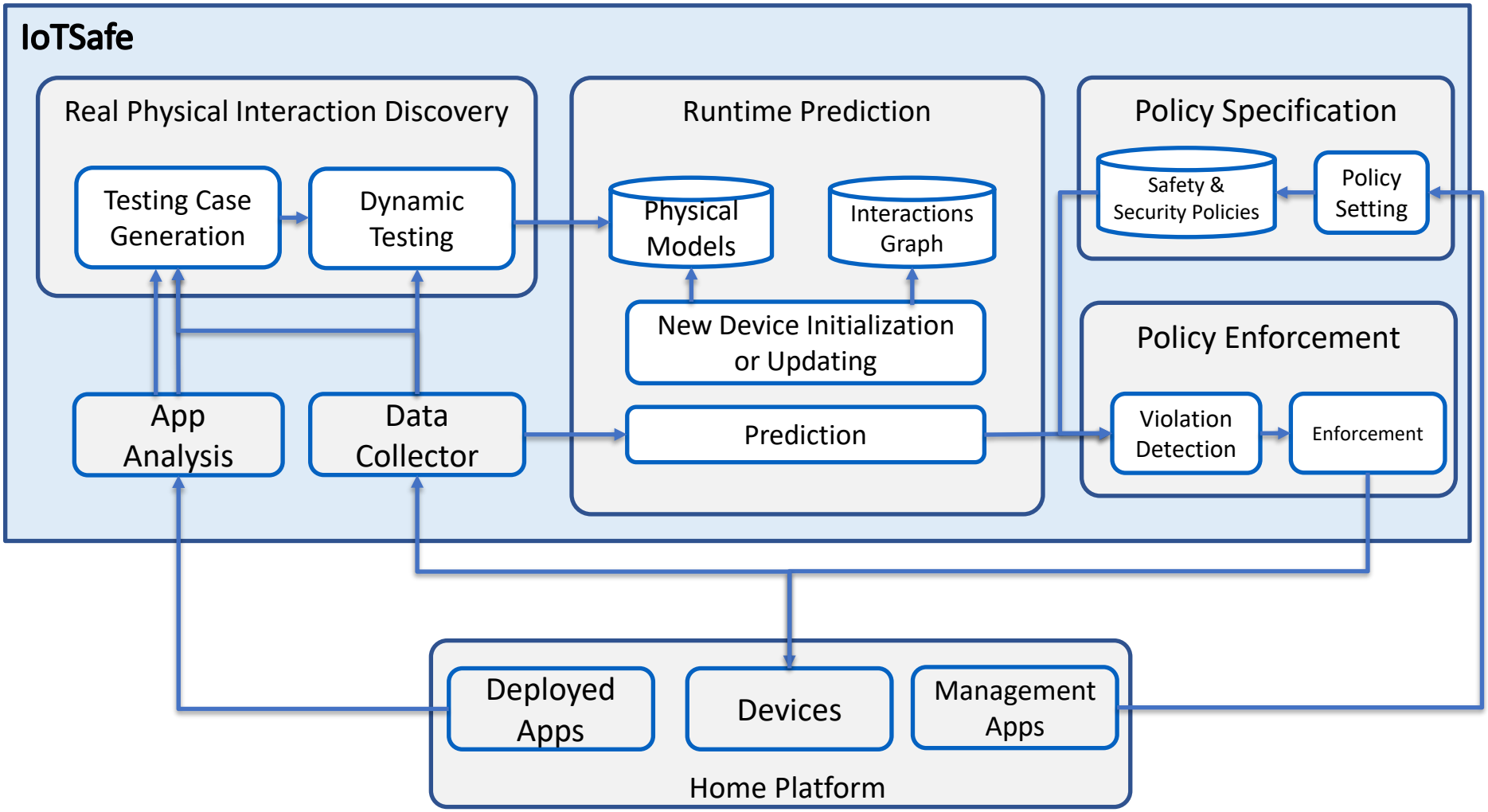
  - Temporal Context

  - Implicit Effect

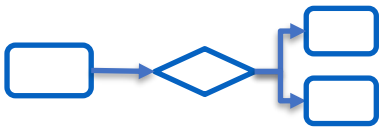


  - Joint Effect

IoTSafe Overview



Testing Case Generation



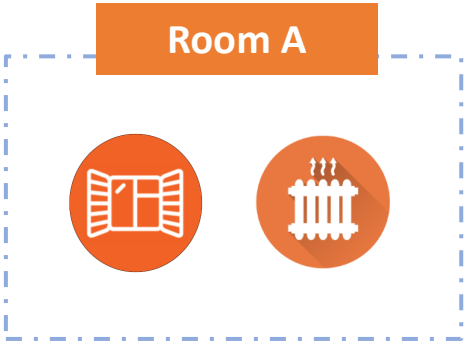
App Control Flows

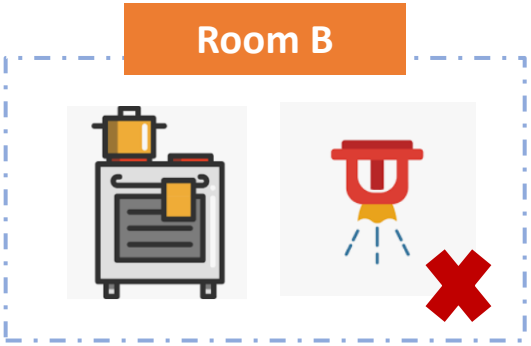
Testing Cases

Room Information

Devices Information

Safety Restriction





Room A

(Heater.on)(Win.close)
(Heater.off)(Win.open)

Room B

(Stove.on)

Dynamic Testing

Cases

Testing

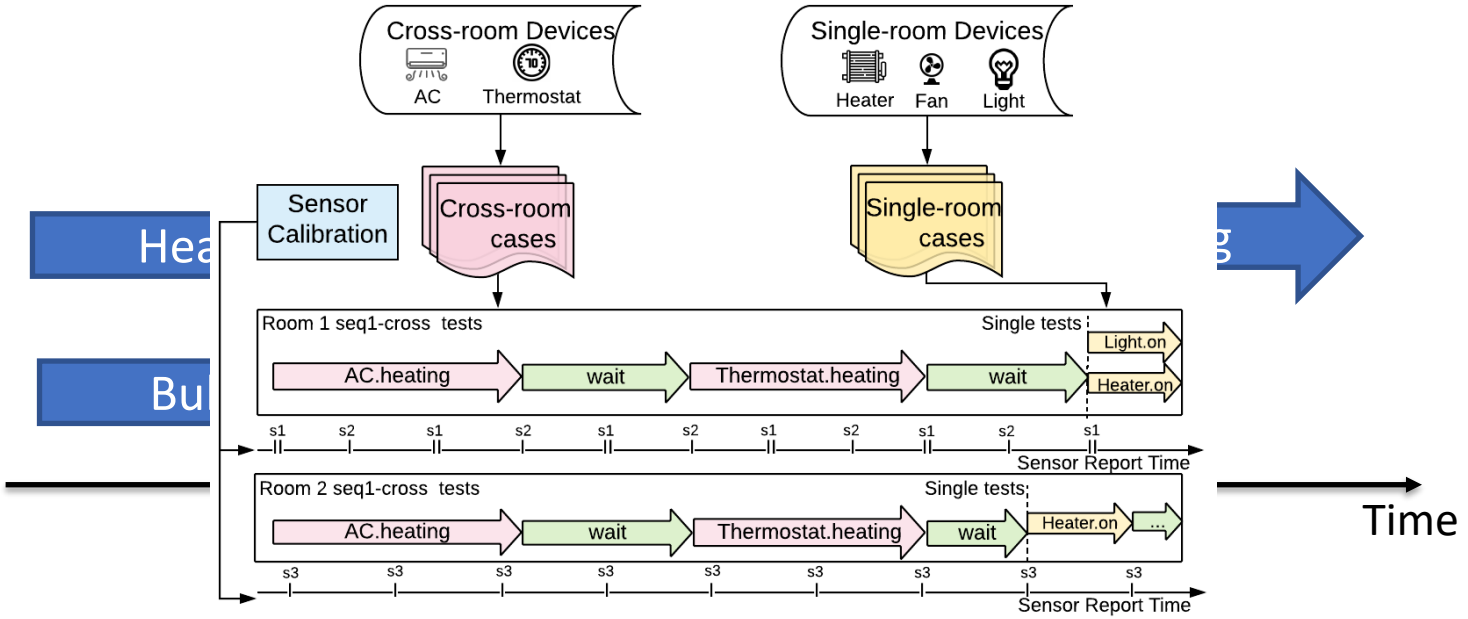
Real Interactions

Physical Models

Sequential Testing

Single-room Parallel

Multiple-room Parallel



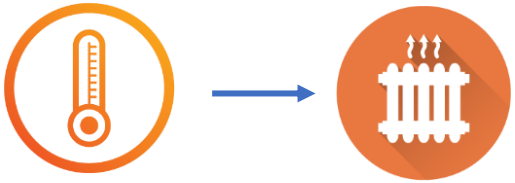
Runtime Prediction

- **Initialize** devices' model based on testing data

Device Data

Violation Block

Data Collector	Physical Model Initialization	Runtime Prediction



$$min \sum_{t} (SensVal(\widehat{D_i}, state, t) - SensVal(D_i, state, t))^2$$

Model Initialization

$$\Delta Q(D_i, state, t_1, t_2)$$

Prediction

Safety & Security Policy

- Policy for Instant Interactions
  - "All electrical appliances cannot be turned on when smoke is detected."
- Policy for Temporal Interactions
  - "Turn off the heater and send a warning when the temperature is above 85F."

More devices?

```
If (device_id ==“Smoke_sensor1”) &&
(Smoke_sensor1.value == “detected”):
    deny(appliances.on);
```

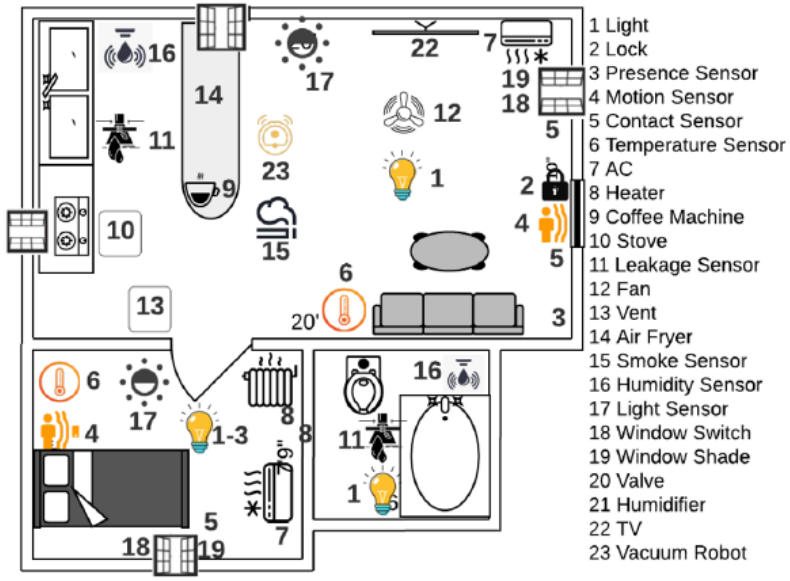
Example of Instant Interaction Control Policy

```
If (device_id ==“Temp_sensor1”) &&
(Temp_sensor1.value > 85 ):
    implement(heater.off);
    implement(push(temperature warning));
```

Example of Temporal Interaction Control Policy

Evaluation Setup

- Apps
  - 21 SmartThings official applications
- Datasets
  - Two real user routine datasets[1][2]
  - 7 groups
- Device
  - Sensors
  - Lock
  - Switches
  - Toaster
  - Heater, AC, Thermostat
  - ...



Testbed for group 4

[1] Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses, IEEE S&P, 2020

[2] How Risky Are Real Users' IFTTT Applets?, SOUPS, 2020

Real Physical Interaction Discovery

- Static Analysis
  - 21 applications in total
  - Seven groups
  - Three groups of real user data

Group ID	Potential Interaction[1]	Real Interaction	FP of Static Analysis	FN of Static Analysis
1	17	12	5	6
2	13	5	8	1
3	41	19	22	9
4	130	39	91	17
5	32	14	18	4
6	46	17	29	8
7	42	22	20	6

Physical Interaction Discovery Results

[1] On the Safety of IoT Device Physical Interaction Control, CCS, 2018

Implicit Interactions

- From 33 devices
  - Y represents real interactions identified by IoTSafe
  - O represents implicit interactions identified by IoTSafe
  - X represents unreal interactions results

Devices	Temperature	Humidity	Smoke	Motion
Thermostat	Y	O		
Radiator	Y	O	X	
Coffee Machine		O		
Kettle		Y		O
Robot				O
Stove	O			
Air Fryer	O	O		

Physical Interaction Discovery Results

Physical Model

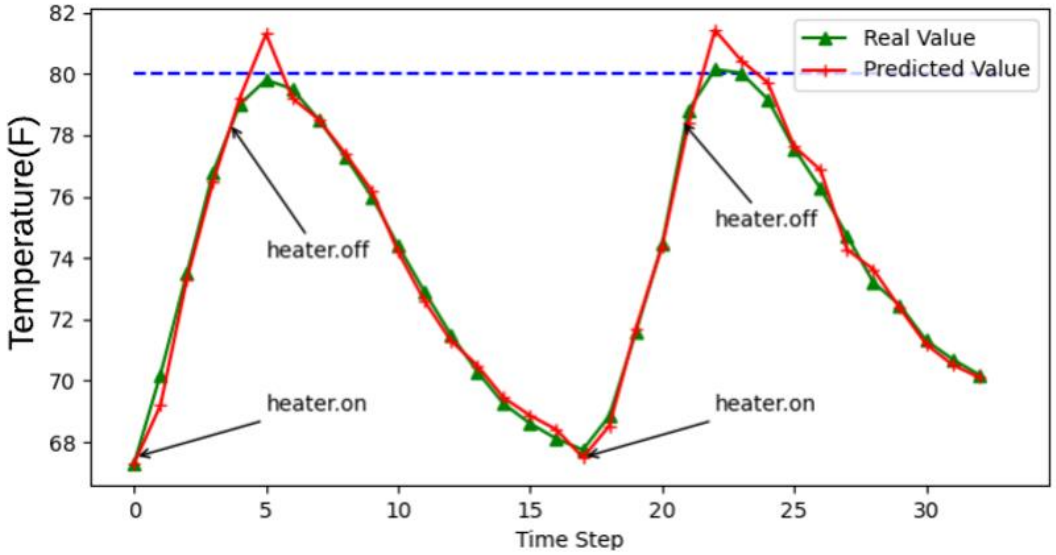
- Channel Specific
  - 3 Physical channels
  - Based on different sensor intervals

Physical Channel	Prediction Lead Time(minute)	Average Error	Error Percentage
Temperature	45	3.3F	4.6%
	30	1.5F	2.1%
	15	1.0F	1.4%
Humidity	45	7.1%	11.8%
	30	3.4%	5.7%
	15	1.3%	2.2%

Average Errors For Two Channels

Runtime Prediction

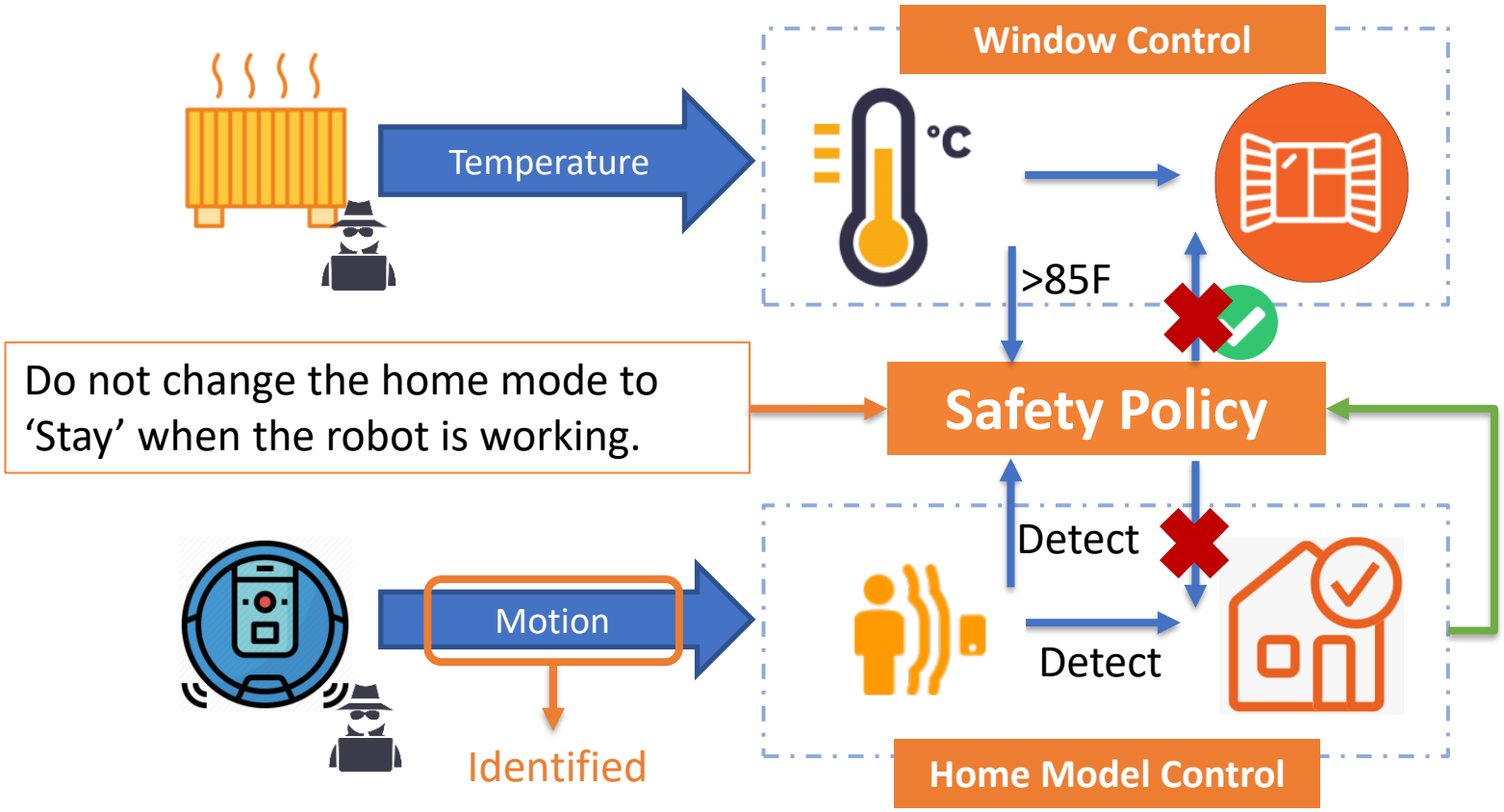
- Temperature
  - 80F as threshold
  - Detected 15 (93%) risky situations based on group 1
- Multiple Channels
  - 12 predefined risky situations
  - Detected 53 (96%) risky situations based on group 4



Effectiveness of Temperature Prediction

Case Study

- Safety/Security Policy
  - Do not open the window if no one is at home.



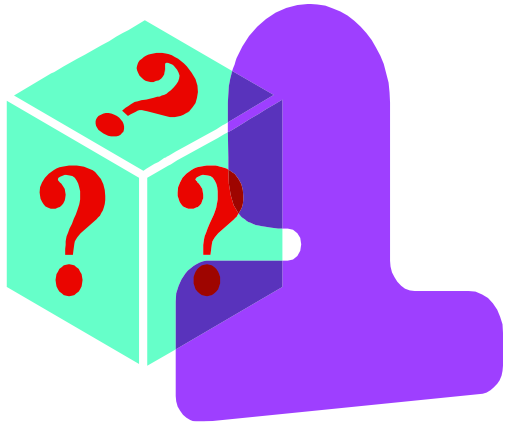
Related Work

System	App Analysis	Real Physical Interaction	Runtime Policy Enforcement	Condition Prediction	Policy Correction
IoTSafe	✓	✓	✓	✓	✓
IoTGuard[NDSS,19]	✓		✓		
Peeves[CCS,19]	✓	✓			
Helion[S&P 20]	✓		✓	✓	
iRuler[SIGSAC,19]	✓				✓
IoTMon[CCS,18]	✓				
HomeGuard[DSN 20]	✓				✓
Menshen[TCPS,18]	✓				✓

Conclusion

- IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery
  - Real physical interaction discovery
  - Runtime modeling and prediction
  - Runtime policy enforcement
- Implementation and Evaluation
  - 7 testbeds;
  - 96% enforcement accuracy
- Future Work:
  - Other prediction/modeling methods
  - Consider human interactions
  - Cross-platform access control

Q & A



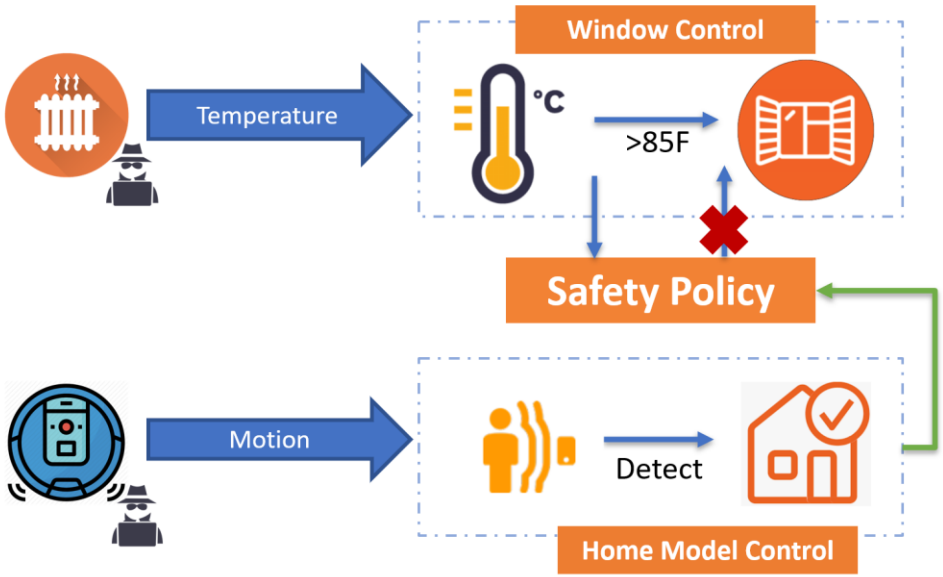
Thank you!

Email: wding@clemson.edu

Threat Model

- Vulnerable or Malicious Applications
  - Design/implementation flaws
  - Code with hidden intentions

- Vulnerable Devices
  - Design flaws

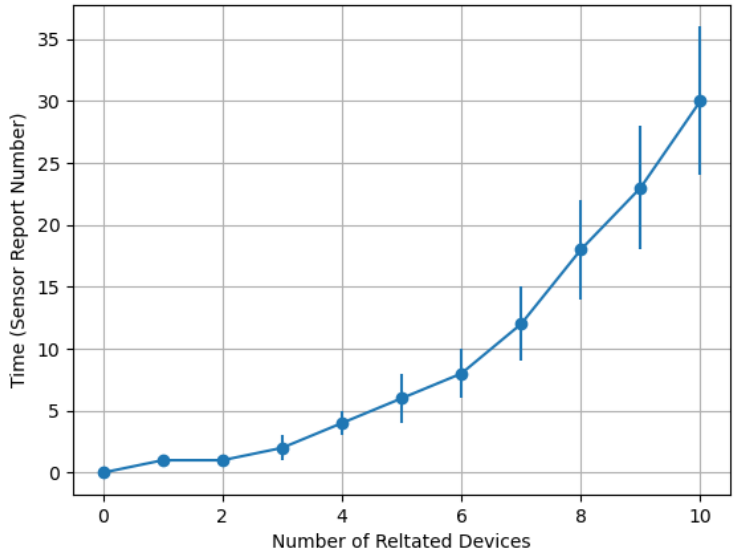


Design Goal

- A system can capture all potential physical interactions and enable policy enforcement
  - capture **real physical interactions** on the platform
  - Build physical **models** for temporal interactions
  - **Predict** physical conditions based on models
  - Enforce policies properly

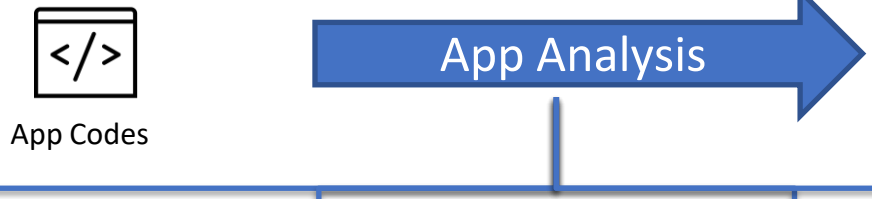
Performance

- Dynamic Testing
  - 40 to 135 minutes
- Runtime Latency
  - Around 230ms
- New Device Initialization
  - 3 related sensor reports



Time consumption of new device initialization

Application Analysis



General Model	AST construction	Traversing & Parsing input section	NLP for physical channel
IFTTT model (IF-This-Then-That) Trigger - Action	AST generated by **Groovy Console**	Extract control flows by tracing **variables & functions**	Identify Channels by **Similarities**