On the Safety of IoT Device Physical Interaction Control

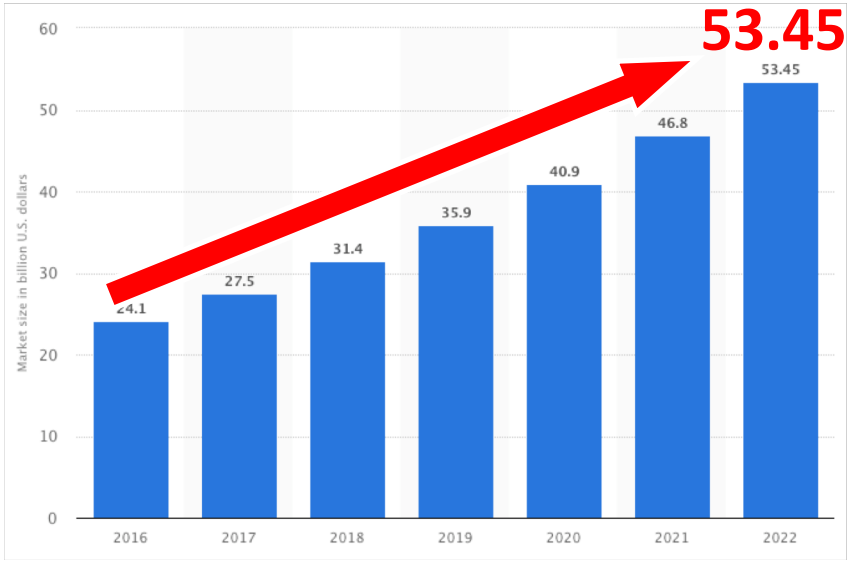
Wenbo Ding Hongxin Hu

CLEMSON UNIVERSITY

CCS 2018

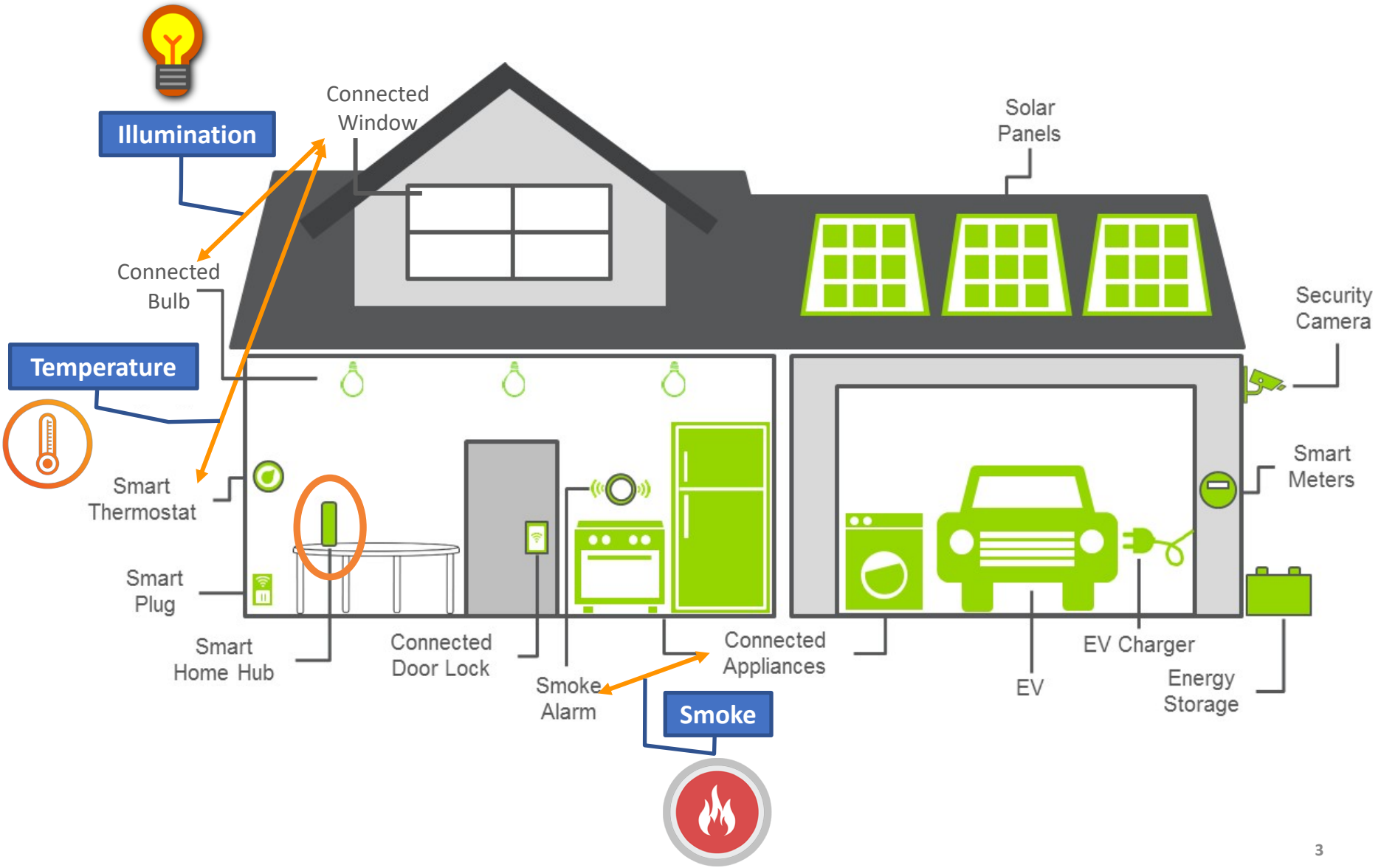
Smart Home Trend

- Huge market size
- Fast-growing amount of devices
- More complicated functions
- Commercial platforms



Global smart home market revenue 2016-2022 (From Statista)

Physical Interaction

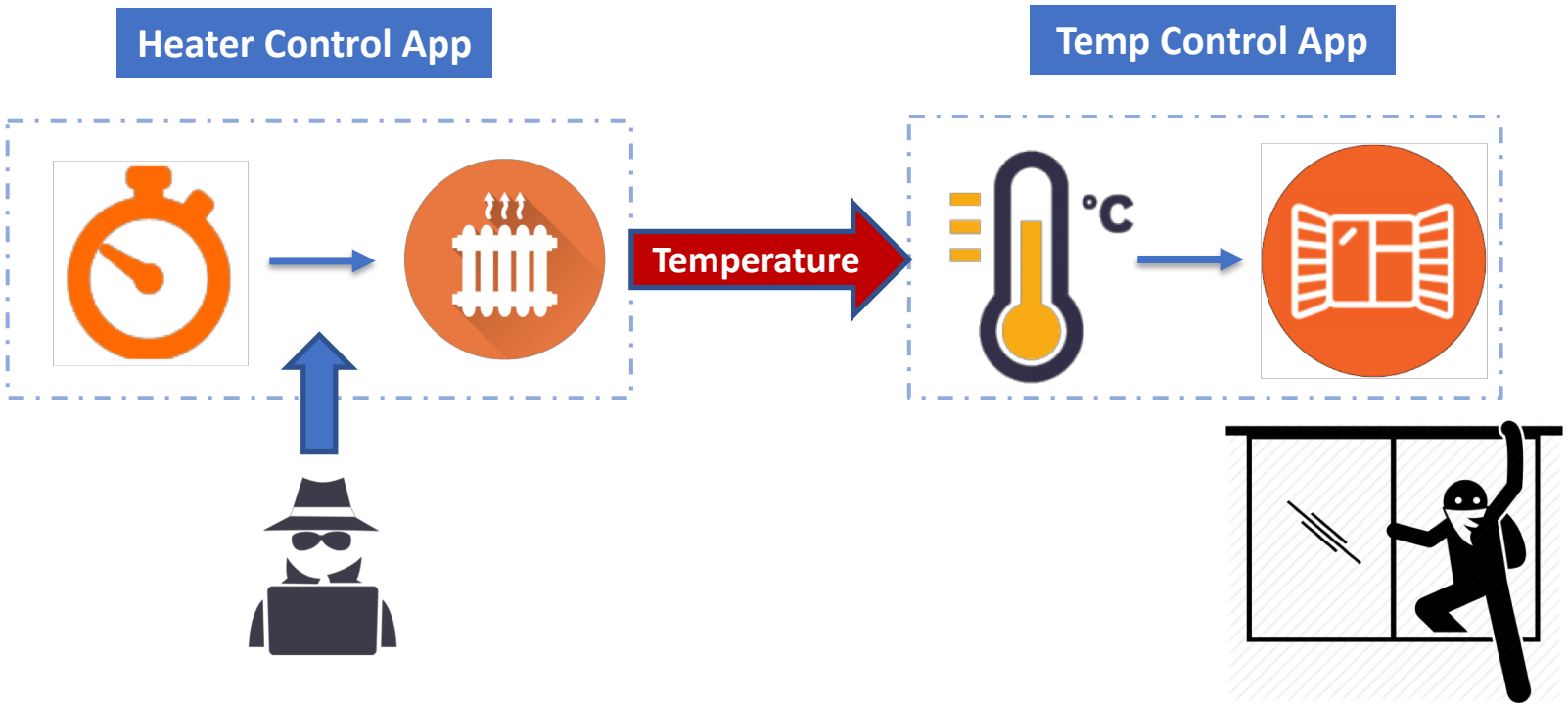


Physical interactions of IoT devices can bring significant convenience to end users

They can also be potentially exploited by attackers

Inter-app Physical Interaction

- Unexpected Interaction

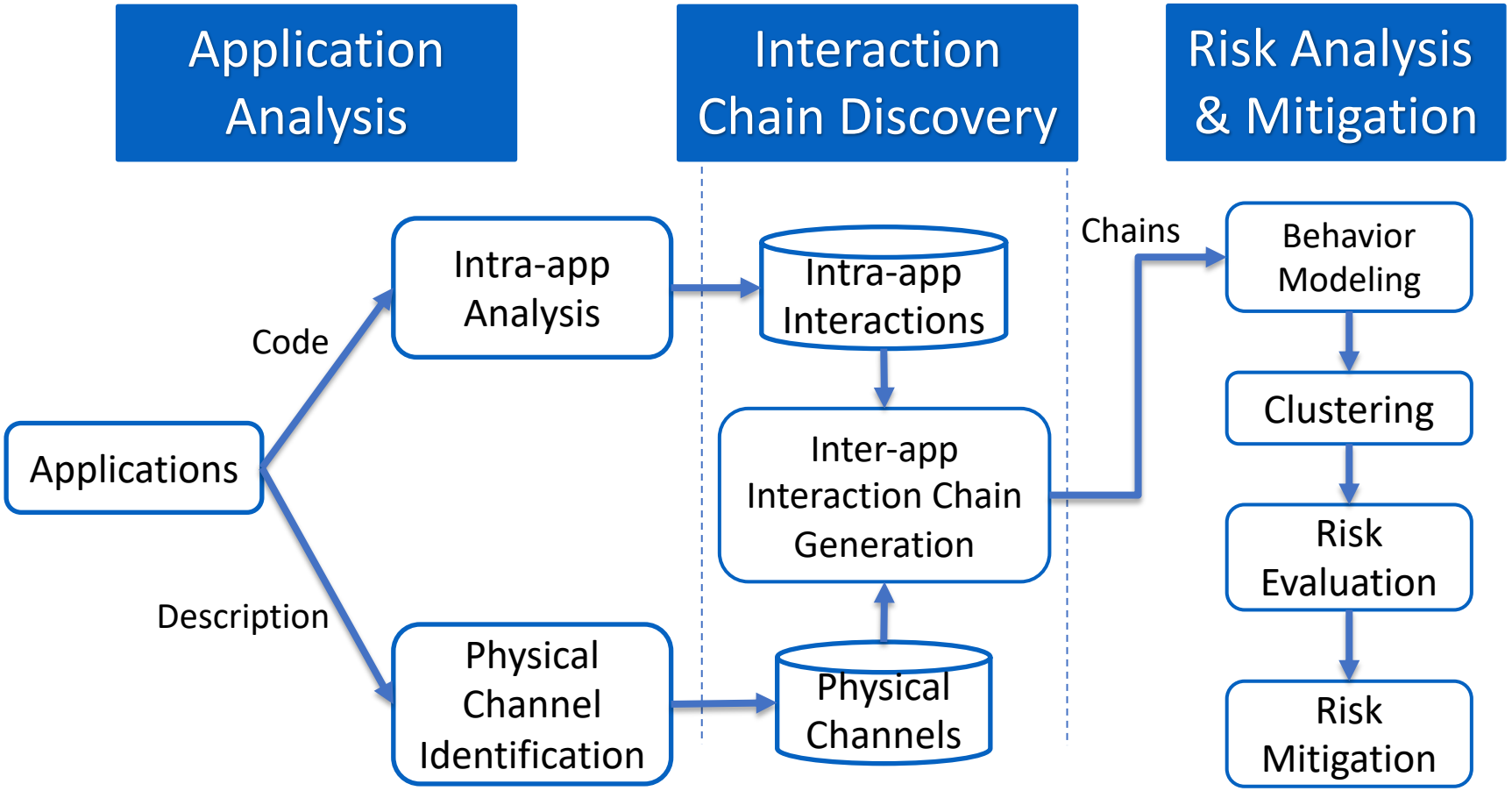


IoTMON captures all potential **physical interactions** and enable **safe interaction controls**

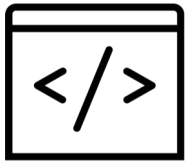
Challenge

- Identification of physical channels
- Identification of inter-application interaction chains
- Risk analysis and mitigation

IoTMON Overview

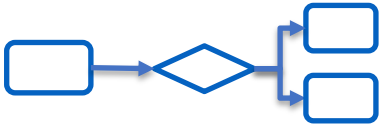


Intra-Application Analysis



App Codes

Static Analysis



Intra-app Interaction

General Model	AST construction	Traversing input section	Tracing functions
IFTTT Trigger-Action	*CompilationUnit* provided by Groovy	Visitor pattern	Related capabilities flows

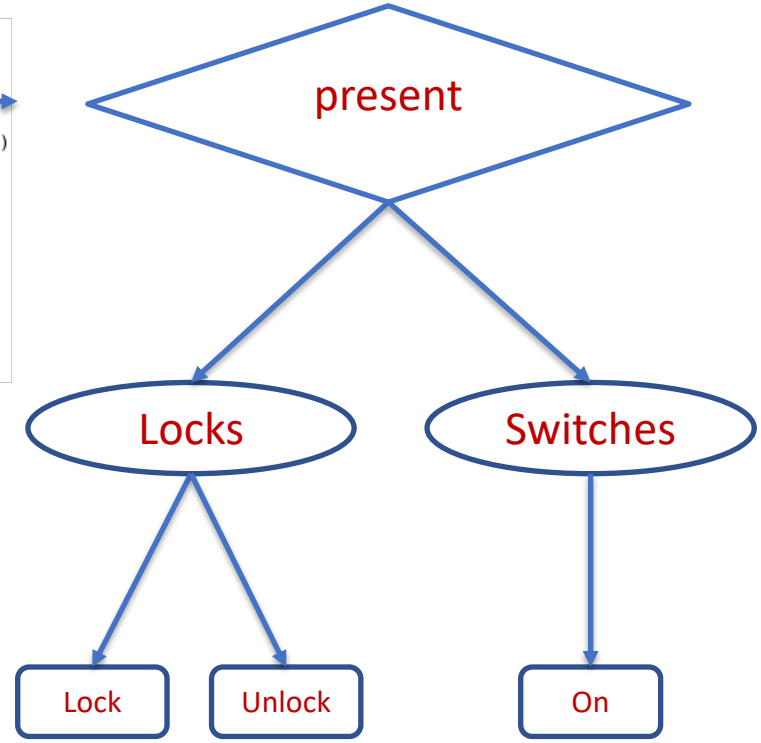
Intra-Application Analysis Example

```
def presence(evt)
{
    if (evt.value == "present") {
        if (unlock == "Yes") {
            def anyLocked = lock1.count{it.currentLock == "unlocked"} != lock1.size()
            if (anyLocked) {
                sendMessage("Doors unlocked at arrival of $evt.linkText")
            }
            lock1.lock()
            lock1.unlock(delay: 10)
            switch1.on(delay: 1000)
        }
    }
```

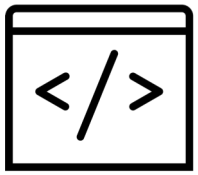
Triggers

"Lock it when I leave"

Actions



Physical Channel Identification



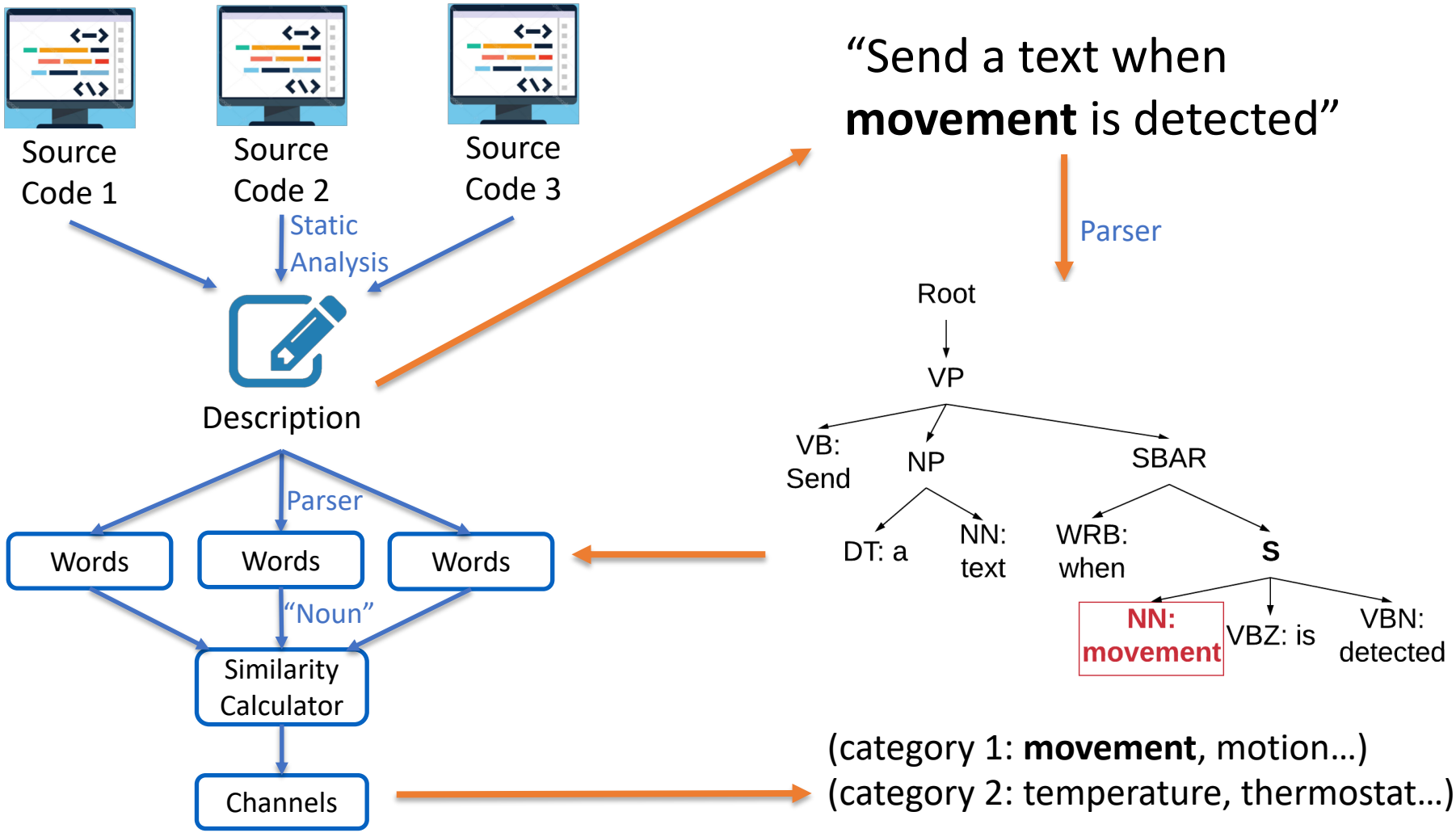
App Description

NLP

Channels

Parser	Key-words Extraction	Words Clustering	Channel Summary
The **Stanford** Parser Tool	Related **Noun**	**Word2Vec**	Words Categories

Physical Channel Identification



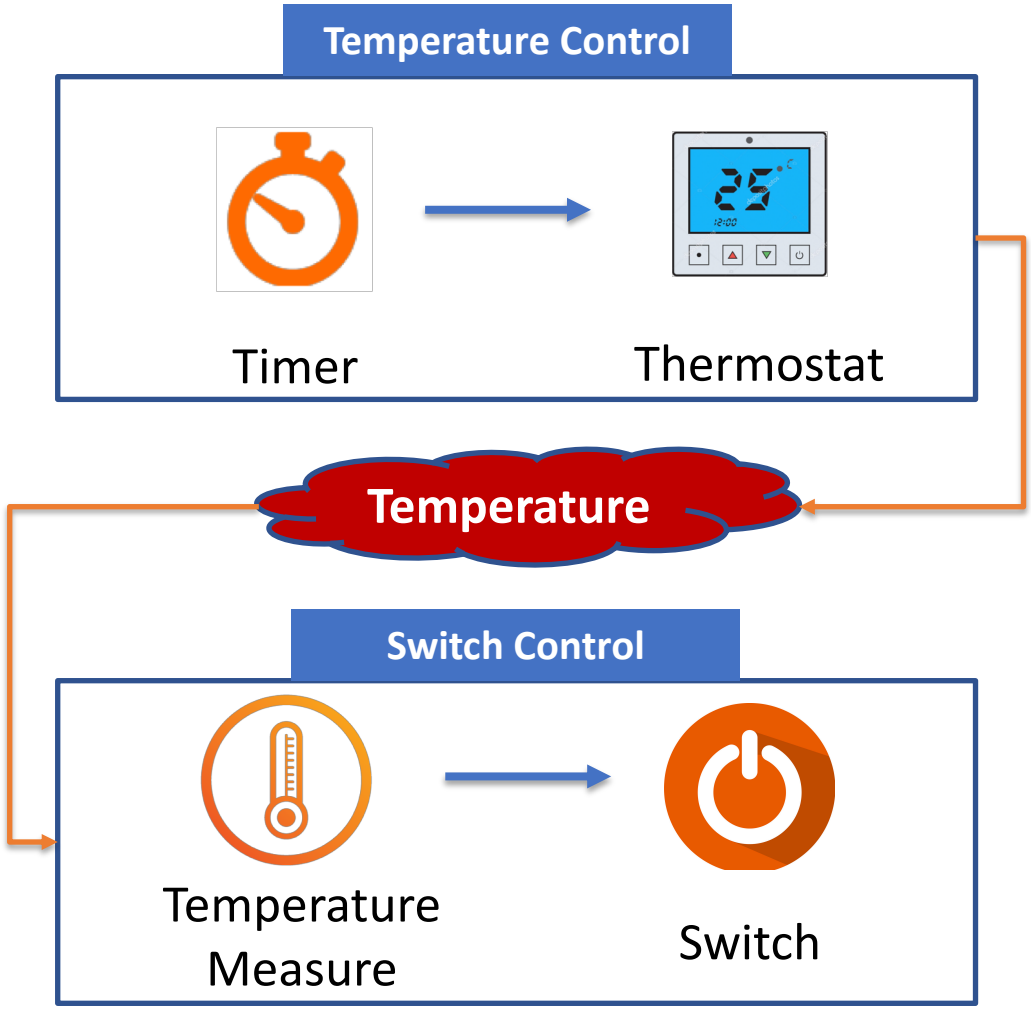
Physical Channel Identification

- Channel Identification
  - 185 official SmartThings applications
  - 124 have physical related functions
  - 7 Physical channels

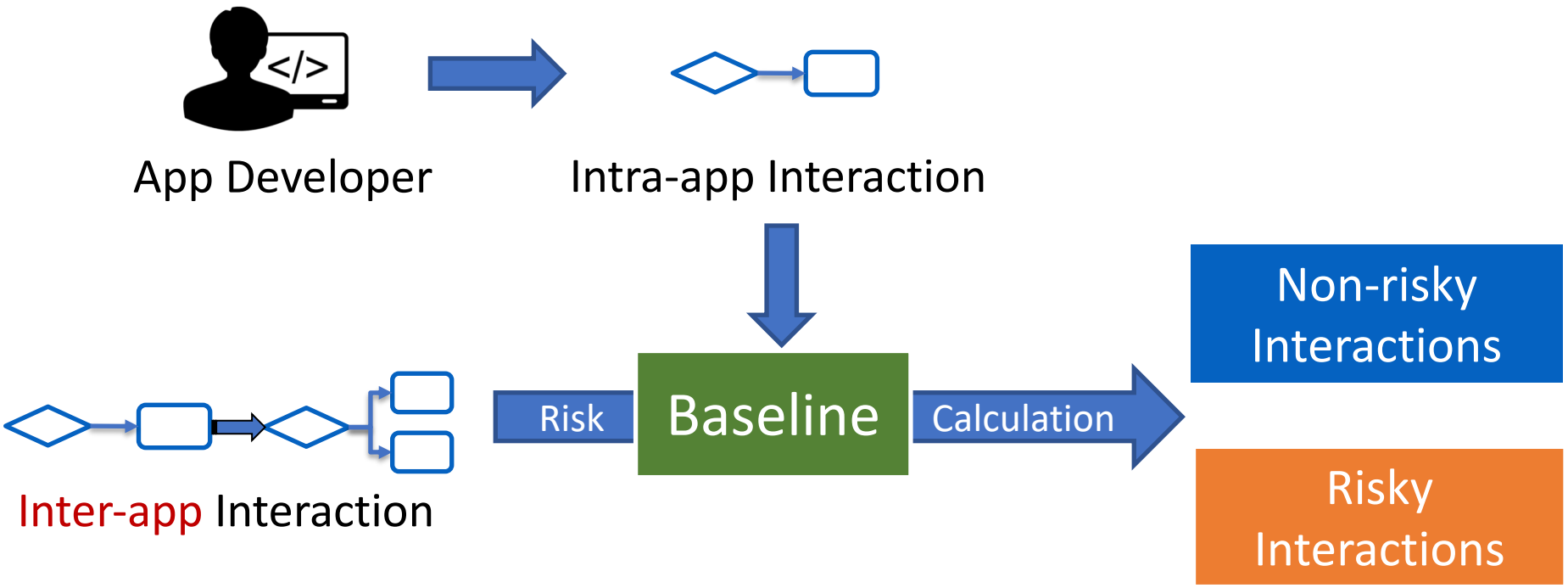
Physical Channel	Example APP	Descriptions
Temperature	Keep Me Cozy	"Changes your thermostat settings."
Humidity	Humidity Vent	"When the humidity reaches a specific…"
Illumination	Brighten Dark Places	"Turn your lights on when a sensor…"
Motion	It Moved	"Send a text when movement is detected"
Location	Lock it When I Leave	"Locks a deadbolt or lever lock when a Presence tag or smartphone leaves a location "
Smoke	Smart Home Monitor	"Monitor Your home for intrusion, fire, carbon monoxide, and more"
Leakage	Flood Alert	"When water is detected…"

Interaction Chain Generation

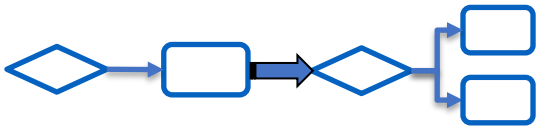
- Input:
  - Intra-app interactions
  - Channels
  - Channel-app relations
- Output:
  - Inter-app interaction chains



Risk Analysis



Baseline Setting



Intra-app Interaction Chain

Baseline

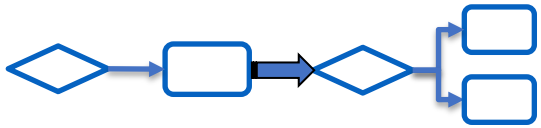
Behavior Modeling

Clustering

Distance Based Modeling

K-Means Clustering

Behavior Modeling



Interaction Chain

Modeling

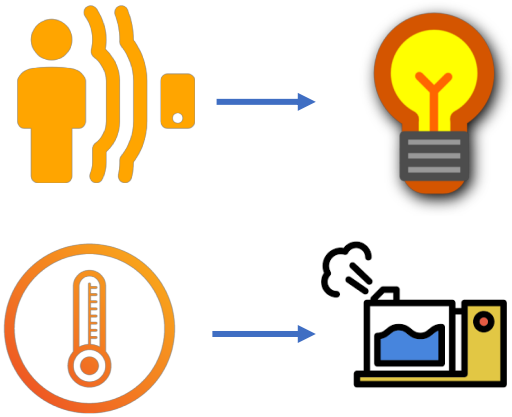
(-15, 30, 0, 0, 0)
(-15, 0, 45, 0, 0)

Interaction Vectors

Intra-app Channel Correlation Discovery

Channel Value Assignment

Mapping



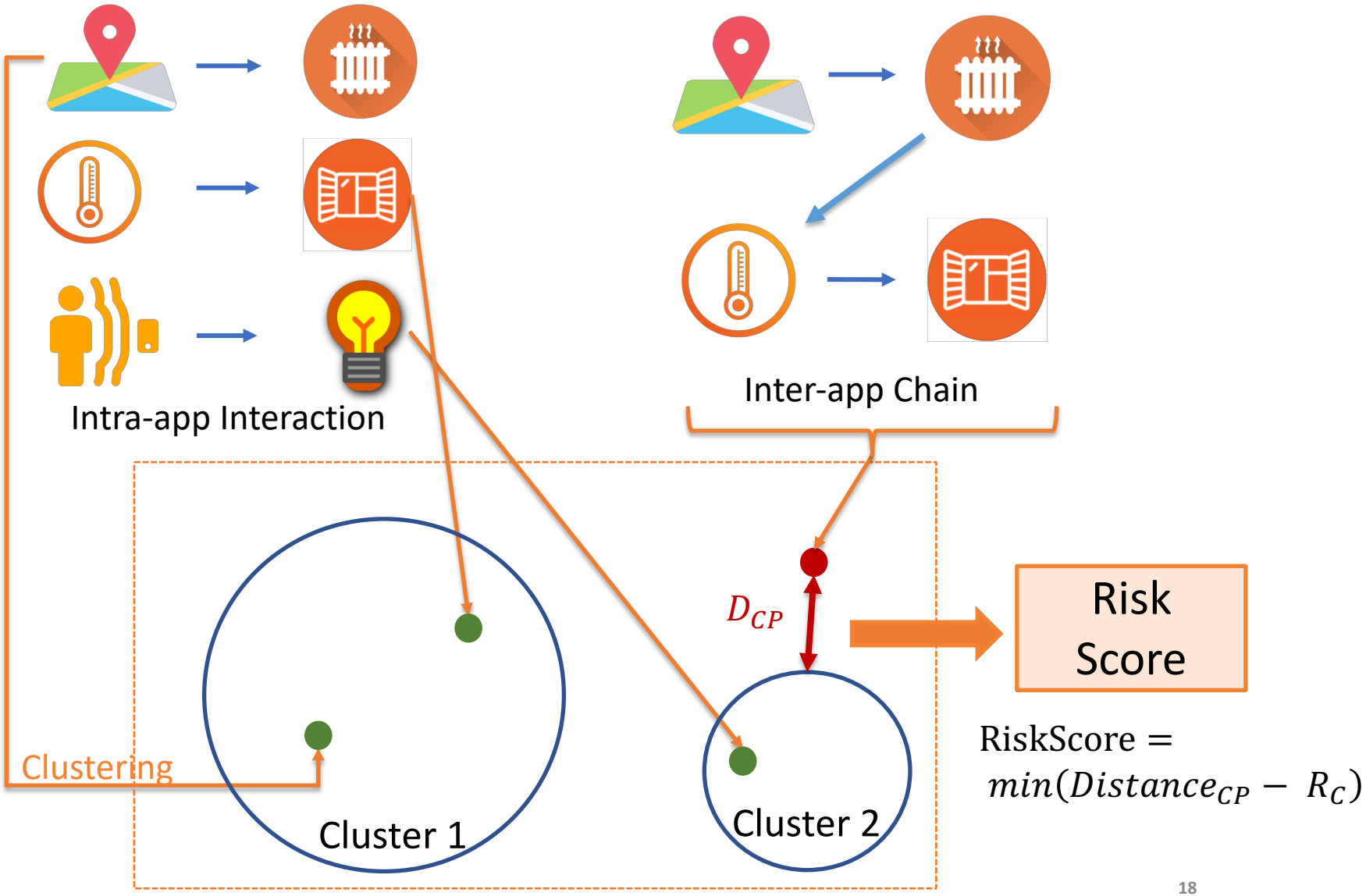
Interactions

(0, 0, 0, 60, -75, 0)

(-15, 30, 0, 0, 0, 0)

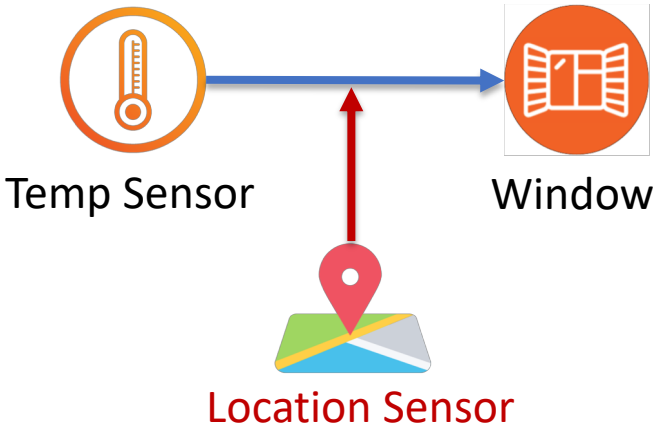
Vectors

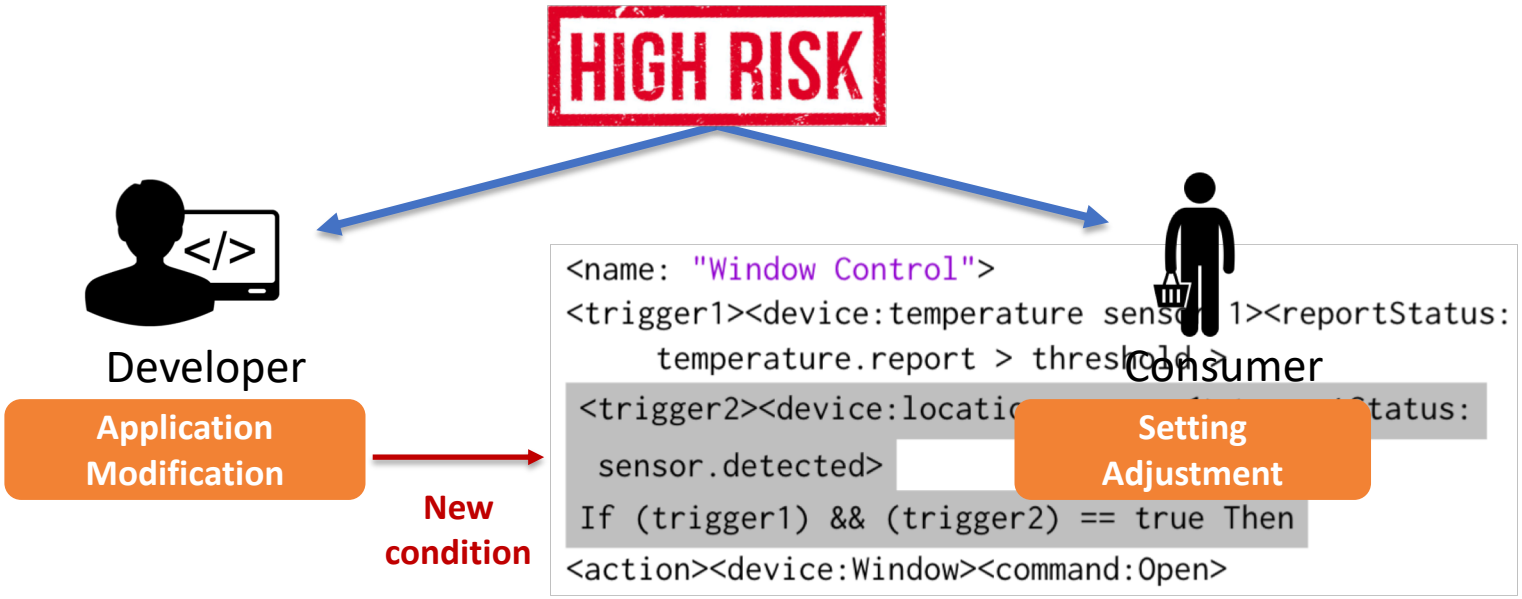
Risk Analysis



Risk Mitigation

- For Developer
  - Application modification
  - Add trigger conditions to applications
- Normal User
  - Change applications settings





Evaluation Setup

- Dataset
  - 185 SmartThings official applications
  - NLP: Word2Vec Google news dataset
- Device
  - Sensors
  - Lock
  - Switches
  - Toaster
  - Heater, AC, Thermostat
  - ...

Intra-app Analysis

- Static Analysis
  - 185 applications
  - 135 can generate control flows

Applications	Triggers (capability)	Actions (capability.command)
Close the valve	waterSensor	valve.close
Its too cold	temperatureMeasure	switch.on
Keep me cozy ii	temperatureMeasure	thermostat.setCoolingpoint
Whole house fan	temperatureMeasure	switch.on
Smart security	motionSensor	Alarm.both

Examples of Intra-app Interactions

Physical Channel Identification

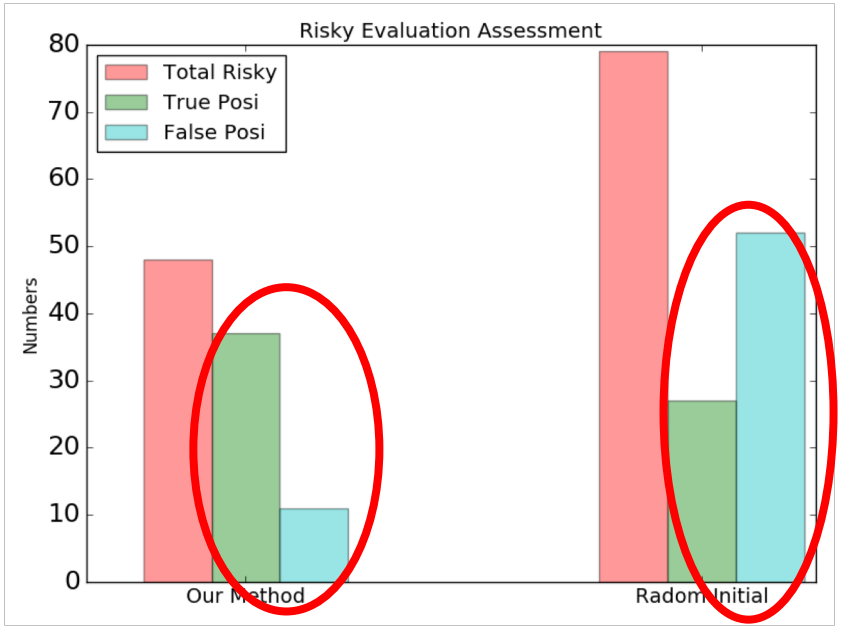
- Channel Identification

Physical Channel	Example Capabilities
Temperature	temperatureMeasurement, thermostat, switch(AC)
Humidity	relativeHumidityMeasurement, switch(vent)
Illumination	illuminanceMeasurement, switch(bulb), switchlevel
Motion	motionSensor, contactSensor, threeAxis
Location	presenceSensor, location
Smoke	carbonDioxide, smokeDetector
Leakage	waterSensor, valve

Physical Channels and Associated Capabilities

Effectiveness of Risk Evaluation

- From 185 applications
  - 162 Inter-application Interactions
  - **37** Risky interactions

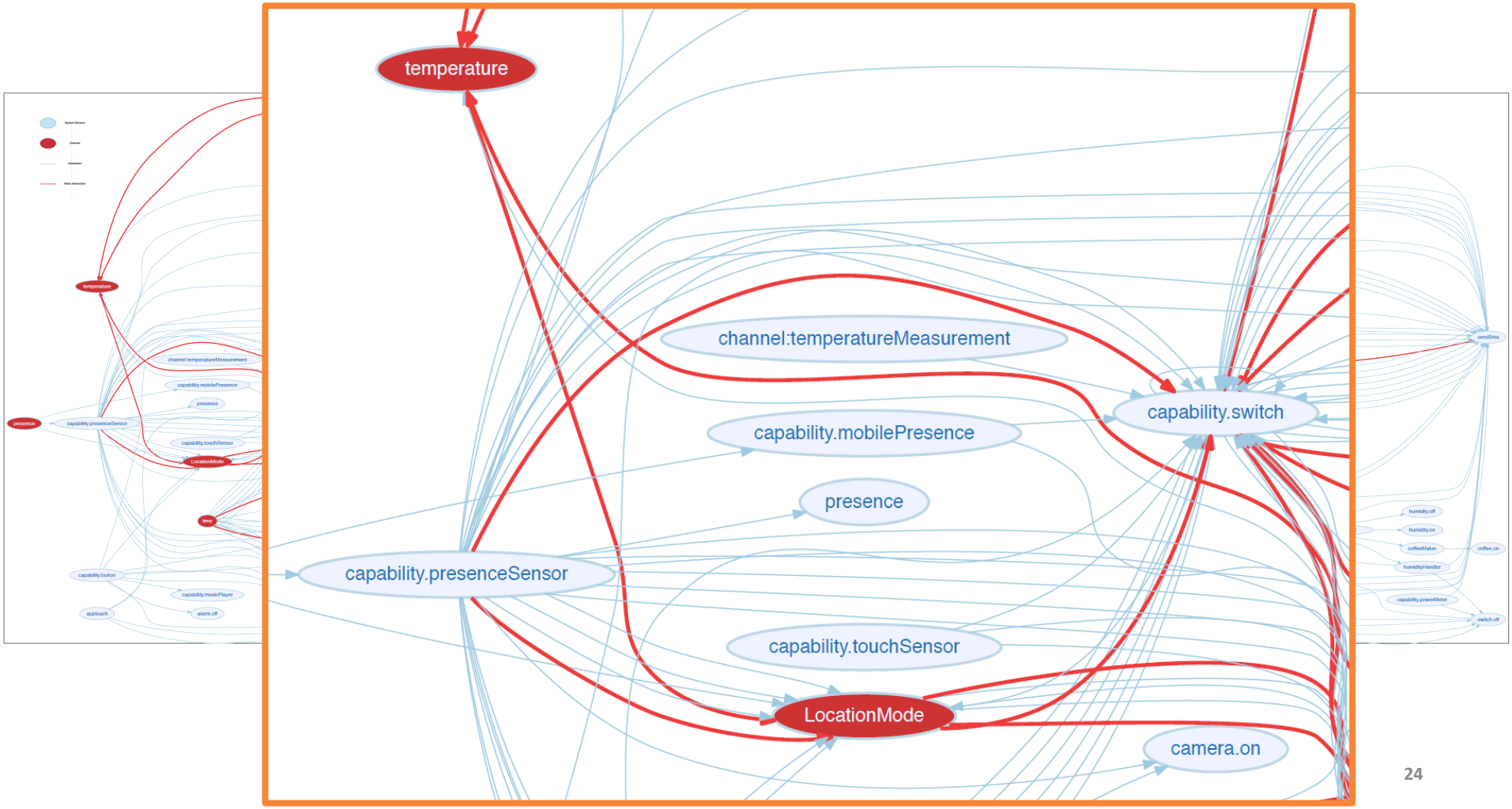


Initialization Method	Total Interaction	Toal Interaction	True Positive	Positive Rate
Our method	162	48	37	**77%**
Random		79	27	**34%**

Result Summary

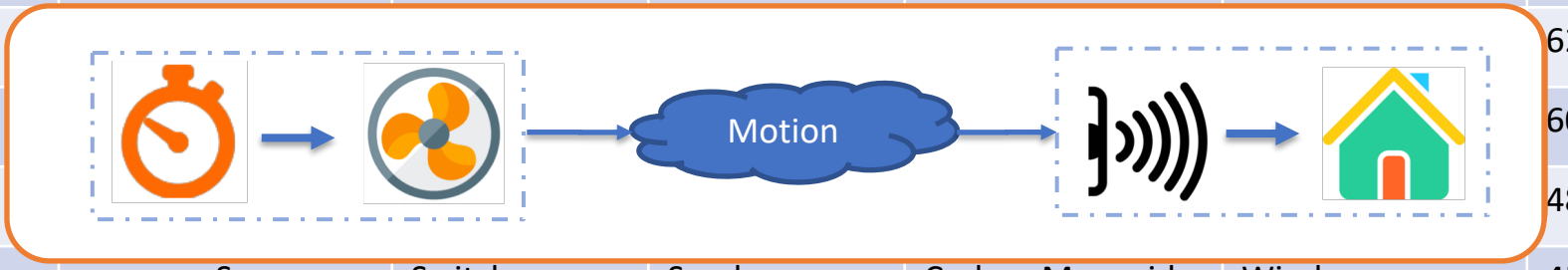
Inter-app Interaction Chain Summary

- **162** potential inter-application interactions
- **37** of 162 are risky interactions



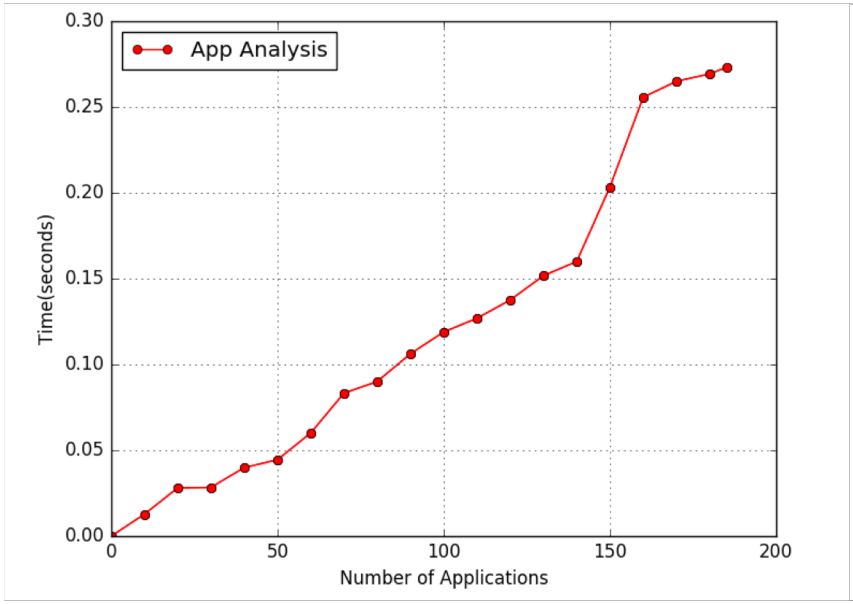
Top 10 High Risk Interactions

No.	Trigger 1	Action 1	Channel	Trigger 2	Action 2	Risk Score
1	Mode	Switch	Smoke	Carbon Monoxide	Lock	70.75
2	Time	Switch	Motion	Motion Sensor	Mode	64.81
3	Time	Mode	System	Mode	Lock	62.92
4						62.75
5						60.01
6						48.74
7	presenceSensor	Switch	Smoke	Carbon Monoxide	Window	45.21
8	Time	Mode	System	Mode	Heater	40.83
9	Time	Mode	System	Mode	Bulb	40.50
10	waterSensor	Bulb	Illuminance	illuminMeasure	Bulb	35.06

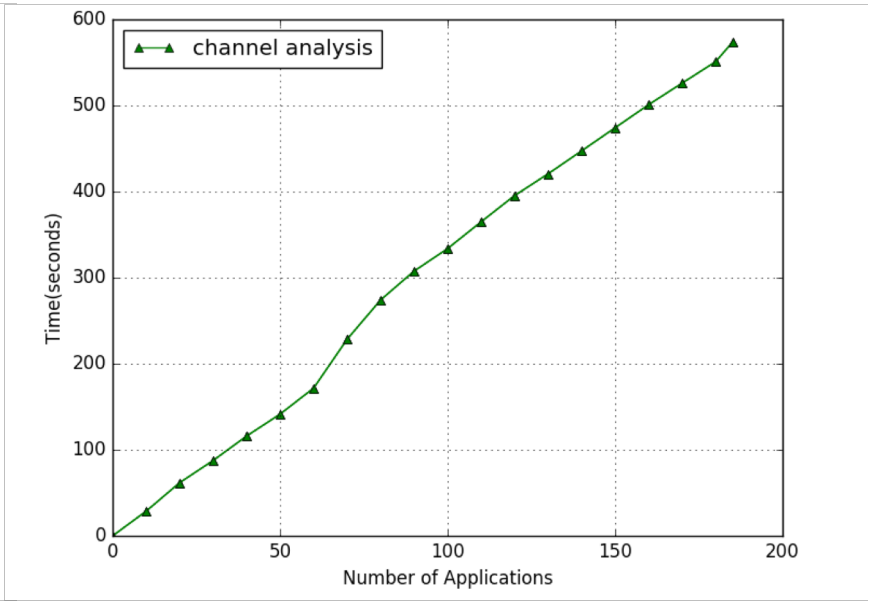


Performance

- Application Static Analysis
  - 0.27s for 185 applications
- Channel Identification
  - Around 580s for 185 applications' descriptions



Application Static Analysis

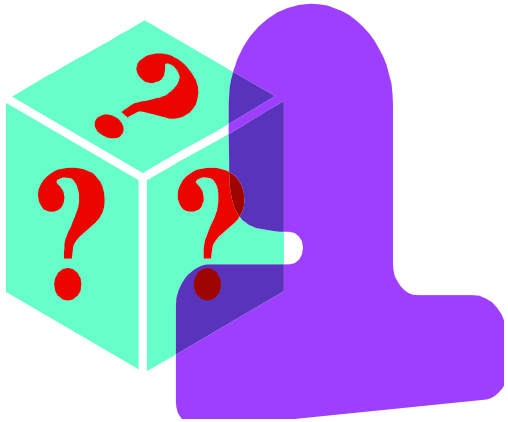


Channel Identification

Conclusion

- IoTMON: physical interaction identification and safe interaction control
  - Physical Channel Identification
  - Inter-application Chain Generation
  - Risk Analysis and Mitigation
- Implementation and Evaluation
  - 7 physical channels; 162 potential chains; 37 high risk interactions
- Future Work:
  - New cross-app attacks
  - Fine-grained mitigation
  - Runtime monitoring

Q & A



Thank you!

Email: wding@clemson.edu

Related Work

- IoT Security:
  - Platform Flaws (e.g. Handling a trillion flaws **[**HotNets'15**]**, Decoupled-IFTTT [NDSS'16])
  - Hardware and Protocol Flaws (e.g. Sivaraman [WiSec' 16], IoT goes nuclear [IEEE S&P' 17])
  - Malware Applications (e.g. Security Analysis of Smart Home [IEEE S&P'16])
- Risk Analysis:
  - Automatic Risk Evaluation: DREBIN [NDSS'14], RiskMon [CODASPY' 14])
  - Description Consistency Checking (e.g. WHYPER [USENIX' 13], Smartauth [NDSS'17])