Trio: Vendor-Independency, Situational Awareness & Behavioral Analysis for Conflict-free Policy Enforcement in Consumer IoT Ecosystems

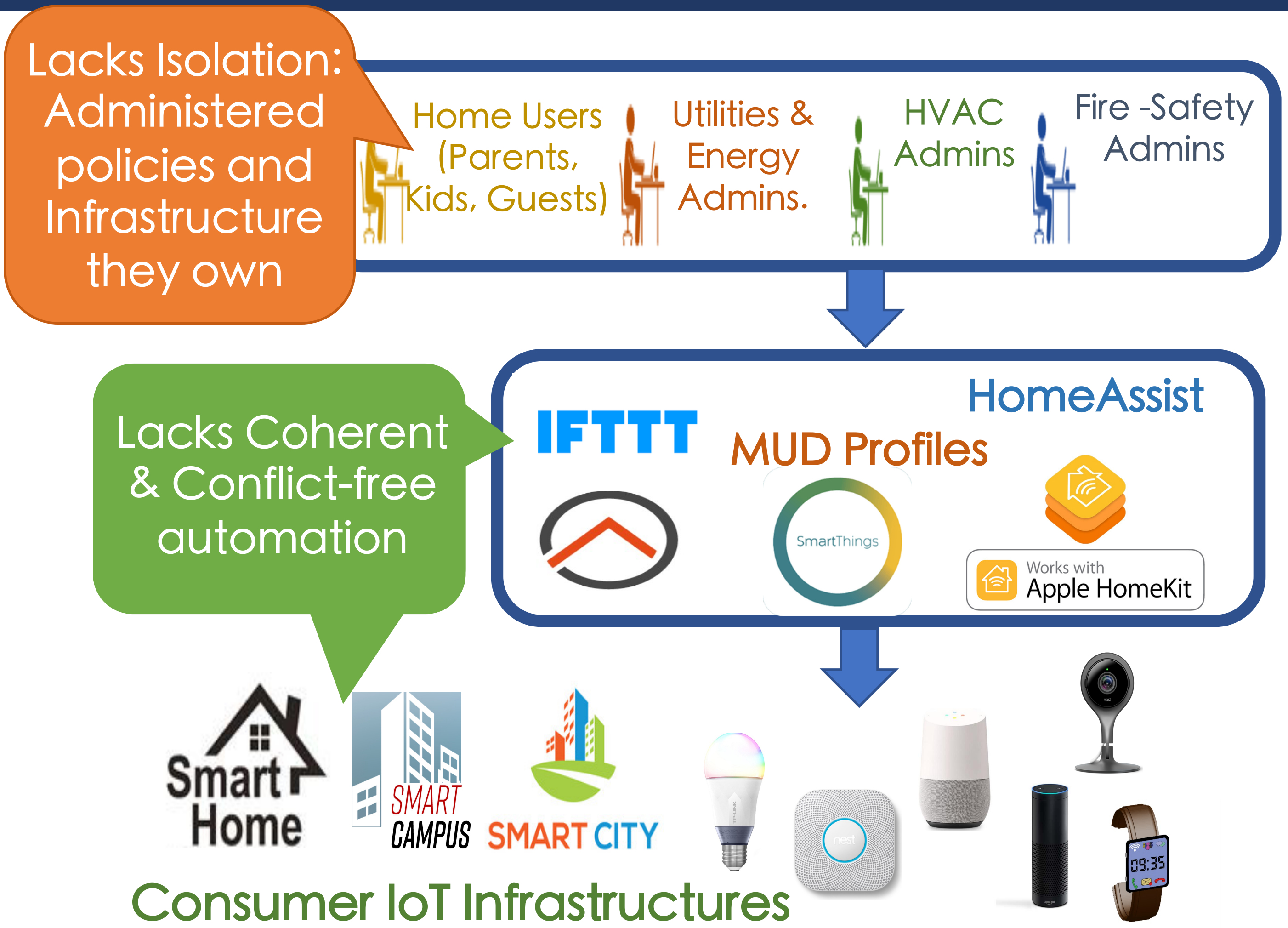
Vasudevan Nagendra

Advisor:

Samir R Das

Stony Brook University

Heterogeneity in Multi-Administrative Consumer IoT



Lacks Isolation: Administered policies and Infrastructure they own

Home Users (Parents, Kids, Guests)

Utilities & Energy Admins.

HVAC Admins

Fire -Safety Admins

Lacks Coherent & Conflict-free automation

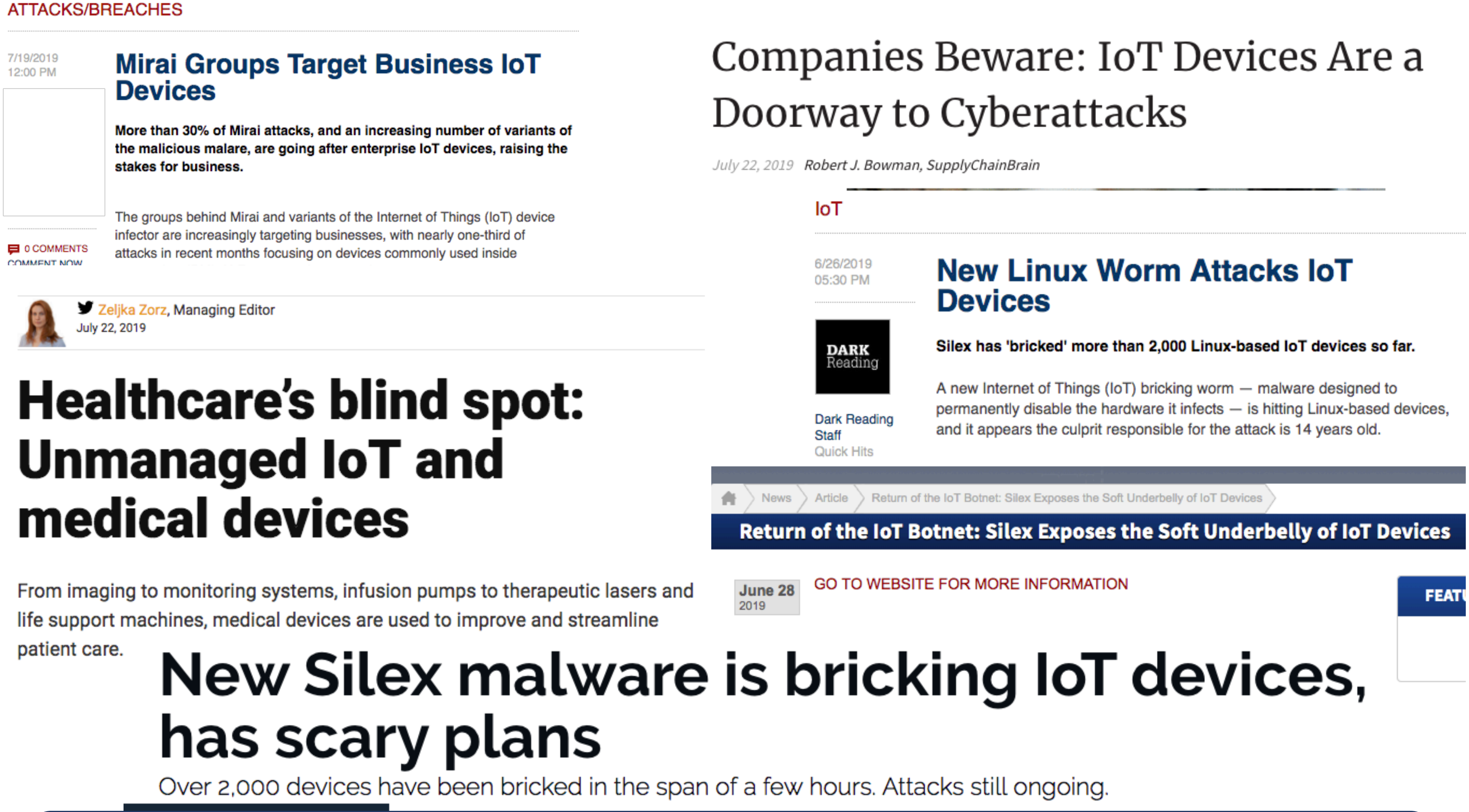
Consumer IoT Infrastructures

__Heterogeneity__:

- Roles in Multi-Administrative domain
- Programming Interfaces
- Automation Frameworks
- Device-types
- Communication Standards
- Device capabilities

Heterogeneity (Roles & Programming Interfaces) makes IoT ecosystem vulnerable and prone to errors

Vulnerable IoT ecosystems



ATTACKS/BREACHES

7/19/2019
12:00 PM

Mirai Groups Target Business IoT Devices

More than 30% of Mirai attacks, and an increasing number of variants of the malicious malare, are going after enterprise IoT devices, raising the stakes for business.

The groups behind Mirai and variants of the Internet of Things (IoT) device infector are increasingly targeting businesses, with nearly one-third of attacks in recent months focusing on devices commonly used inside

0 COMMENTS
COMMENT NOW

Companies Beware: IoT Devices Are a Doorway to Cyberattacks

July 22, 2019 Robert J. Bowman, SupplyChainBrain

IoT

6/26/2019
05:30 PM

New Linux Worm Attacks IoT Devices

Silex has 'bricked' more than 2,000 Linux-based IoT devices so far.

A new Internet of Things (IoT) bricking worm — malware designed to permanently disable the hardware it infects — is hitting Linux-based devices, and it appears the culprit responsible for the attack is 14 years old.

DARK Reading

Dark Reading Staff
Quick Hits

Zeljka Zorz, Managing Editor
July 22, 2019

Healthcare's blind spot: Unmanaged IoT and medical devices

From imaging to monitoring systems, infusion pumps to therapeutic lasers and life support machines, medical devices are used to improve and streamline patient care.

News › Article › Return of the IoT Botnet: Silex Exposes the Soft Underbelly of IoT Devices

Return of the IoT Botnet: Silex Exposes the Soft Underbelly of IoT Devices

June 28
2019

GO TO WEBSITE FOR MORE INFORMATION

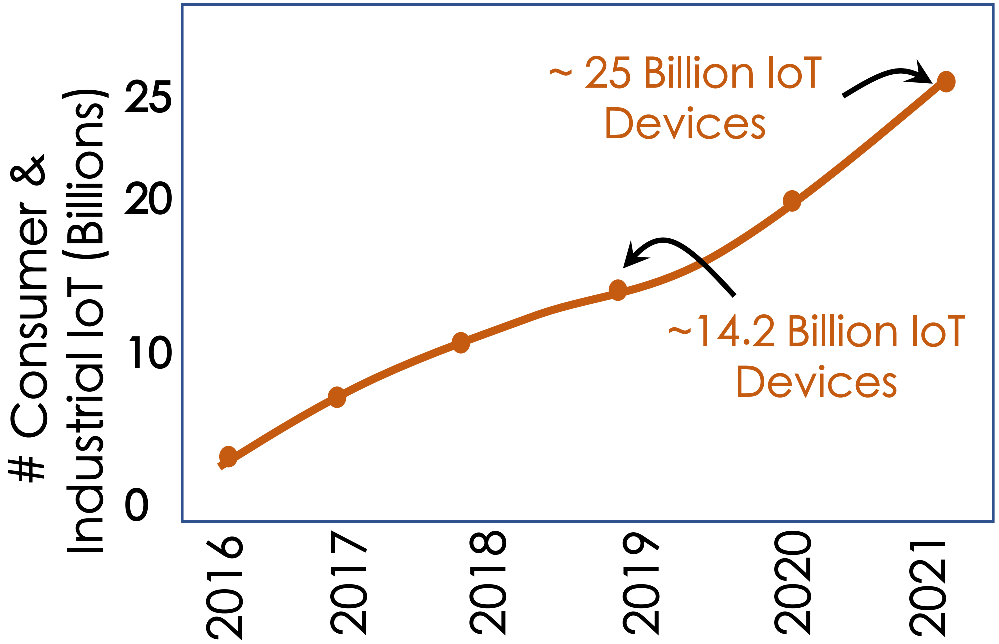
FEATU

New Silex malware is bricking IoT devices, has scary plans

Over 2,000 devices have been bricked in the span of a few hours. Attacks still ongoing.

Lack of Visibility, Coherent Automation and policy enforcement makes IoT ecosystem Vulnerable

Scale contributing to complexity



Consumer IoT:

Fastest growing IoT Vertical

Data Courtesy: Gartner, report Jan 2017, The 2020 total of IoT devices installed across the world will be more than twice this year's.

Data Courtesy: Gartner, report Nov 2018, Gartner Identifies Top 10 Strategic IoT Technologies and Trends https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

Securing IoT infrastructures, Coherent automation & Programmability a challenging with Scale

Challenge (1): Unique Programming requirements

Home Users

Infrastructure Admins

HVAC Admins

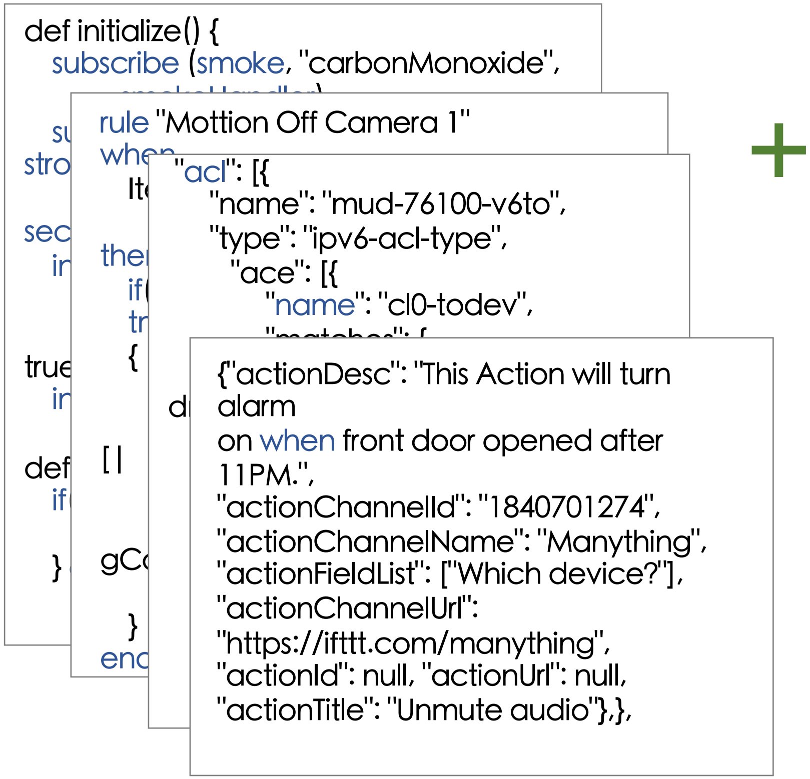
Fire -Safety Admins

IoT Ecosystems Programming Requirements are Unique:

- Location-specific
  - Building/Floor
- Device-type & Capabilities
  - HVACs/Cameras/Lighting
- Vendor-specific
  - Groovy, OpenHAB, MUD, HomeAssist, IFTTT
- Role-based
  - Parental/Kids/Guest

Current Market not matching consumer needs.

Challenge (2): Coherent Automation with heterogeneous IoT apps & Interfaces



```
def initialize() {
   subscribe (smoke, "carbonMonoxide",
   su
stro

sec
   in

true
   in

def
   if

   }
```

```
rule "Mottion Off Camera 1"
when
   It

then
   if(
   tr
   {

[|

gC

   }
end
```

```
"acl": [{
   "name": "mud-76100-v6to",
   "type": "ipv6-acl-type",
     "ace": [{
        "name": "cl0-todev",
d
```

```
{"actionDesc": "This Action will turn
alarm
on when front door opened after
11PM.",
"actionChannelId": "1840701274",
"actionChannelName": "Manything",
"actionFieldList": ["Which device?"],
"actionChannelUrl":
"https://ifttt.com/manything",
"actionId": null, "actionUrl": null,
"actionTitle": "Unmute audio"},},
```

Groovy-based SmartThings

OpenHAB

IFTTT Applet

MUD Profile

+

Web-based Interfaces

- Neither Intuitive Nor Expressible
- Realizing Coherent, Conflict/Violation-free Automation is a tedious

Vendor-Independency is challenging with heterogeneous programming specifications prone to errors

Challenge (3): Infrastructure Isolation & Delegation

Home Users

Infrastruc ture Admins

HVAC Admins

Fire -Safety Admins

Fundamental Isolation/Delegation Limitations:

- Admins/Users ability to delegate control
  - Parents to Kids and Guests
- Isolate Infrastructures they control.
- Leads to data leaks, Rogue Policies, Policy Violations and conflicts.

Infrastructure Admin

E1: Fire Alarm -> Share feed to authorized Fire-personnel

Video-feed

X

Revoke

Lack of Isolation and ability to delegate responsibilities leads to Security, Safety and Privacy concerns

Challenge (4): Conflicts & Violations with multi-administrative domains (1)

SMART CAMPUS

Fire-safety Admin

E1: Fire Alarm -> Share feed to authorized Fire-personnel

Video-feed

Infrastructure Admin

E2: Do not share feed with anyone after 10PM or on week ends

X

Video-feed

Conflict1: >10PM and On week ends in case of fire incident ?

Leads to Safety Violation

Collaborative automation In multi-administrative domain is challenging (could lead to violations)

Challenge (4): Conflicts & Violations with multi-administrative domains (2)

Few Common Smart-Home Automation Conflicts:

Conflicts among Parent and kids in accessing personal room camera?

Conflicts among Parents and kids policy on access to main door entry after 11PM ?

Smart Home

Collaborative automation In multi-administrative domain is challenging (could lead to violations)

Challenge (4): Conflicts & Violations with multi-administrative domains (3)

SMART CAMPUS

Smart Home

Automation Rule (1):

- After 6PM ->
  - Turn ON Bed Room Light
  - Close Blinds

Automation Rule (2):

- Fire event (Fire-alarm=ON):
  - Open Bed Room Windows
  - Open Blinds
  - Open Main Doors
  - …

Automation Rule (3):

- If it Rains:
  - Close Bed Room Windows
  - Leave Blinds Open

Automation Rule (4):

- If blinds are closed:
  - Automatically close Windows

Automation Rule (5):

- If highly humid outside:
  - Close Windows
  - Turn ON AC

Challenge (4): Conflicts & Violations with multi-administrative domains (4)

SMART CAMPUS

Smart Home

Scenario (1):

At 5.55, Fire event happened:

- Automation Rule (2) executed
  “Opened Windows/Blinds”

At 6PM:

- Automation Rule (1) executed
  “Closed Windows”

Outcome: Closes Windows / Blinds during Fire event (Safety Violation)

Challenge (4): Conflicts & Violations with multi-administrative domains (4)

SMART CAMPUS

Smart Home

Scenario (2):

If rain and Fire-incident happens together:

- Conflicting Actions between Rules 2 & 3

Outcome: Closes Windows / Blinds during Fire event (Safety Violation)

Challenge (4): Conflicts & Violations with multi-administrative domains (4)

Scenario (3):
Sequence in which events occur

- 2 Followed by 3 or 4 or 5 is "Unsafe"
- 3 or 4 or 5 followed by 2 is "OK"

Outcome: Incoherent automation (Safety Violation)

SMART CAMPUS

Smart Home

For conflict/violation resolution:
Temporal, Spatial, Sequence of events etc., are key aspects to consider (i.e., Awareness to situation)

Challenge (5): Gap in Automation

- 9AM to 9PM: HVAC Fan speed Level 3 / Light = ON in BLDG1
- 9PM to 6AM: HVAC Fan speed 2/ Light = OFF in Floor2
- 6AM to 9AM: HVAC Speed & Light in Floor 2 and (BLDG1 - Floor2) = ?

Outcome: Gap in Automation
Especially Temporal & Spatial rules
resulting in Unpredicted Behavior

SMART CAMPUS Smart Home

Realizing Coherent conflict-free automation is challenging with simple conflict detection and resolution

Existing Solutions

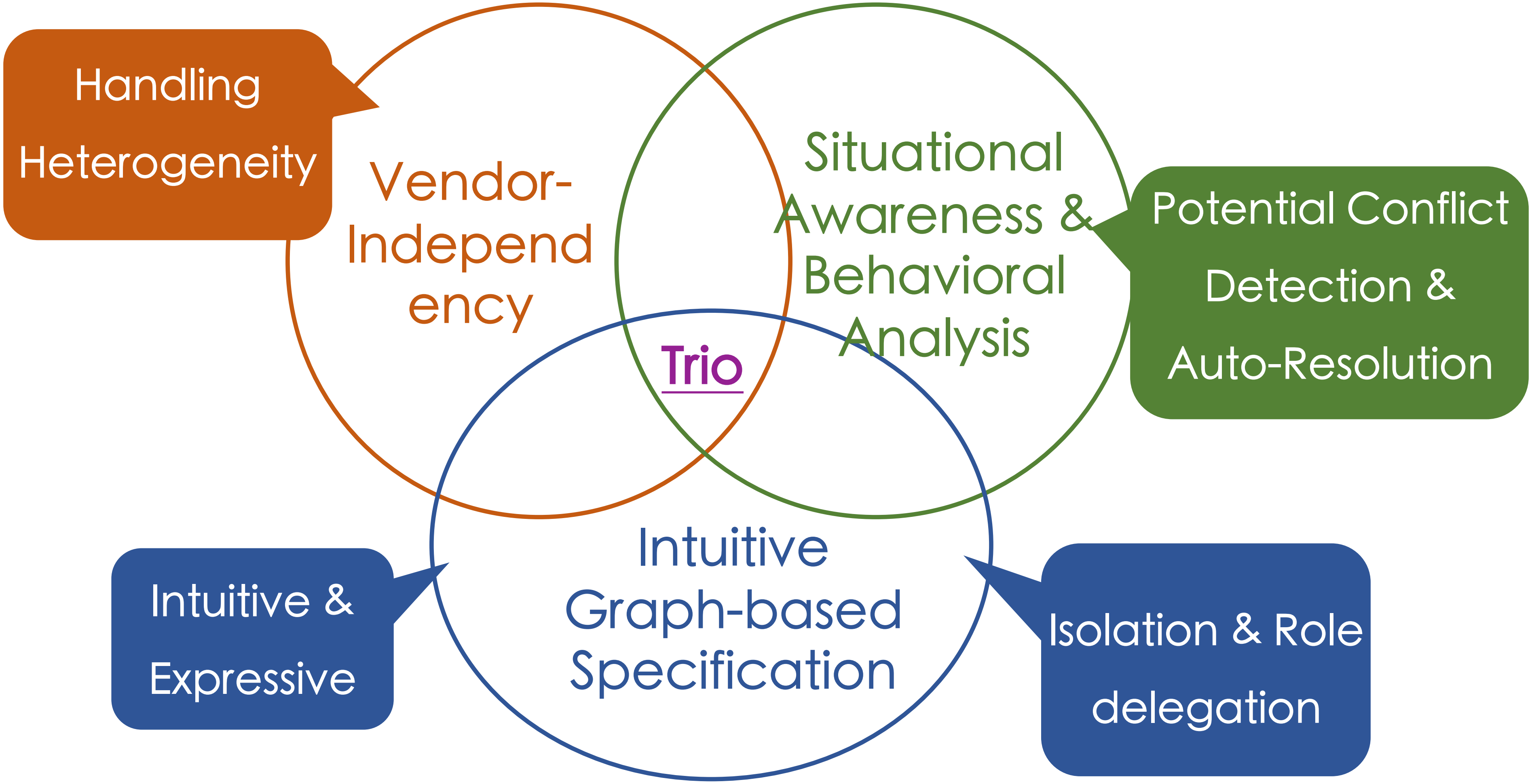
- Detects Static conflicts in IoT programs

- Detects run policy violations, but:
  - Limited in their capabilities,
  - Not scalable
  - Requires code instrumentation
    - Instrumentation could lead to new errors

- Lacks the Context
  - Awareness about the Situations for better violation resolution

Detects wide range of conflicts & violations

Our Approach: Trio



Handling Heterogeneity

Vendor-Independency

Situational Awareness & Behavioral Analysis

Potential Conflict Detection & Auto-Resolution

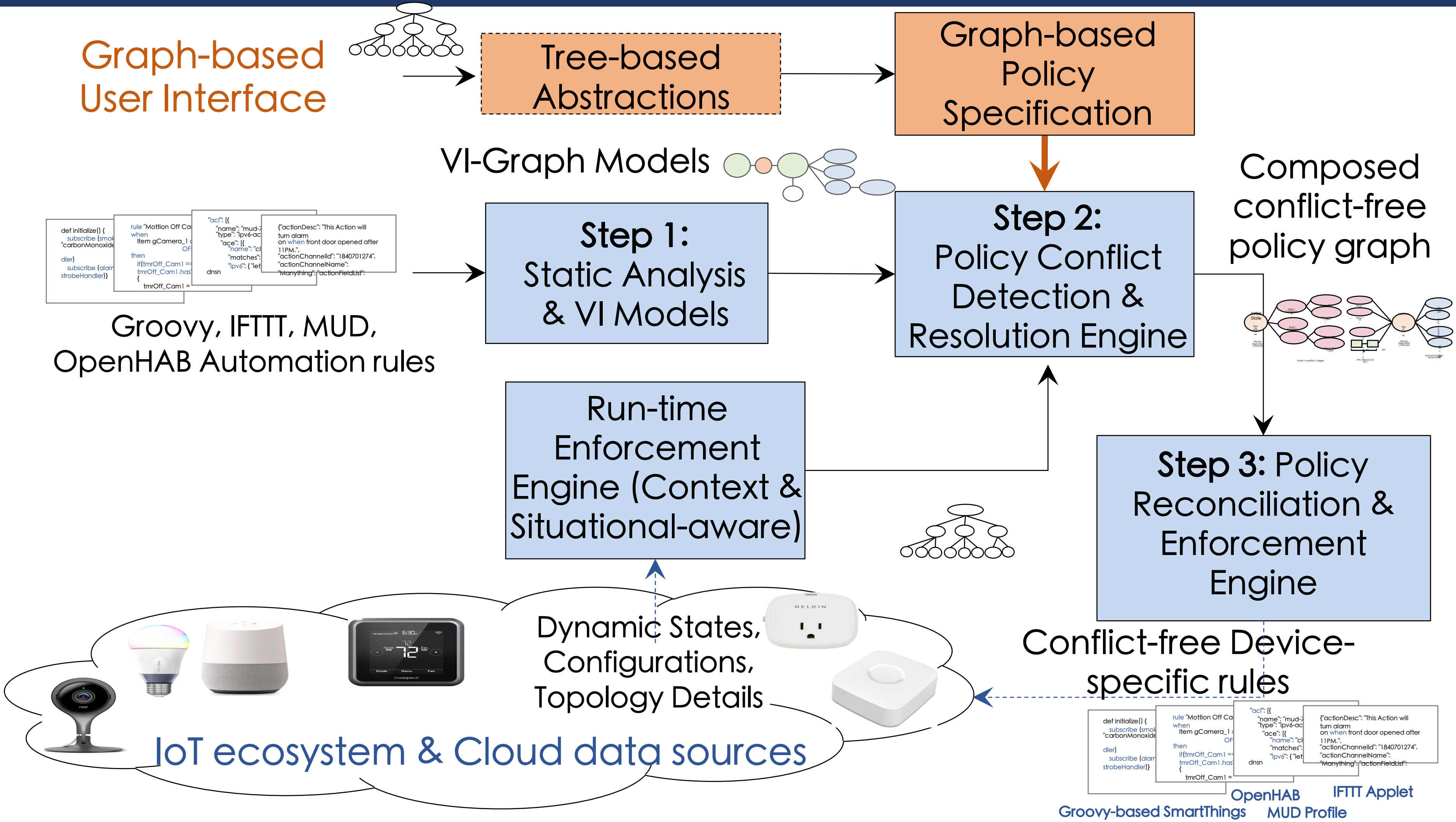
Trio

Intuitive & Expressive

Intuitive Graph-based Specification

Isolation & Role delegation

Our Approach:
(VI Model + Graph-based Specification)



Graph-based User Interface

Tree-based Abstractions

Graph-based Policy Specification

VI-Graph Models

```
def initialize() {
   subscribe (smok
"carbonMonoxide

dler)
   subscribe (alarn
strobeHandler)}
```

```
rule "Mottion Off Ca
when
   Item gCamera_1 c
                    OF
then
   if(tmrOff_Cam1 ==
   tmrOff_Cam1.has
   {
      tmrOff_Cam1 =
```

```
"acl": [{
   "name": "mud-7
   "type": "ipv6-ac
     "ace": [{
        "name": "cl
        "matches":
        "ipv6": { "iet
dnsn
```

```
{"actionDesc": "This Action will
turn alarm
on when front door opened after
11PM.",
"actionChannelId": "1840701274",
"actionChannelName":
"Manything","actionFieldList":
```

Groovy, IFTTT, MUD, OpenHAB Automation rules

Step 1: Static Analysis & VI Models

Step 2: Policy Conflict Detection & Resolution Engine

Composed conflict-free policy graph

Run-time Enforcement Engine (Context & Situational-aware)

Step 3: Policy Reconciliation & Enforcement Engine

Dynamic States, Configurations, Topology Details

Conflict-free Device-specific rules

```
def initialize() {
   subscribe (smok
"carbonMonoxide

dler)
   subscribe (alarn
strobeHandler)}
```

```
rule "Mottion Off Ca
when
   Item gCamera_1 c
                    OF
then
   if(tmrOff_Cam1 ==
   tmrOff_Cam1.has
   {
      tmrOff_Cam1 =
```

```
"acl": [{
   "name": "mud-7
   "type": "ipv6-ac
     "ace": [{
        "name": "cl
        "matches":
        "ipv6": { "iet
dnsn
```

```
{"actionDesc": "This Action will
turn alarm
on when front door opened after
11PM.",
"actionChannelId": "1840701274",
"actionChannelName":
"Manything","actionFieldList":
```

Expressibility, Vendor-Independency & Context

Questions?

Feel free to contact Vasudevan Nagendra
vnagendra@cs.stonybrook.edu

Stony Brook University

Our Initial Work:
VISCR: Intuitive & Conflict-free Automation for Securing the Dynamic Consumer IoT Infrastructures
Vasudevan Nagendra, Arani Bhattacharya, Vinod Yegneswaran, Amir Rahmati, Samir R Das.
https://arxiv.org/abs/1907.13288 ArXiv:1907.13288, July 2019.