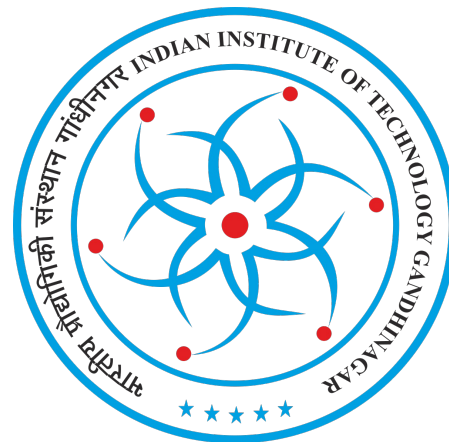


# Towards Usable Security Analysis Tools for Trigger-Action Programming

**McKenna McCall**, Eric Zeng, Faysal Hossain Shezan, Mitchell Yang, Lujo Bauer, Abhishek Bichhawat, Camille Cobb, Limin Jia, Yuan Tian

**Carnegie  
Mellon  
University**

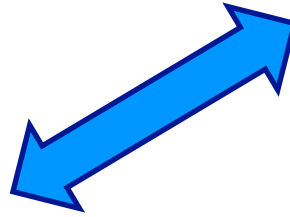


UNIVERSITY OF  
**ILLINOIS**  
URBANA-CHAMPAIGN

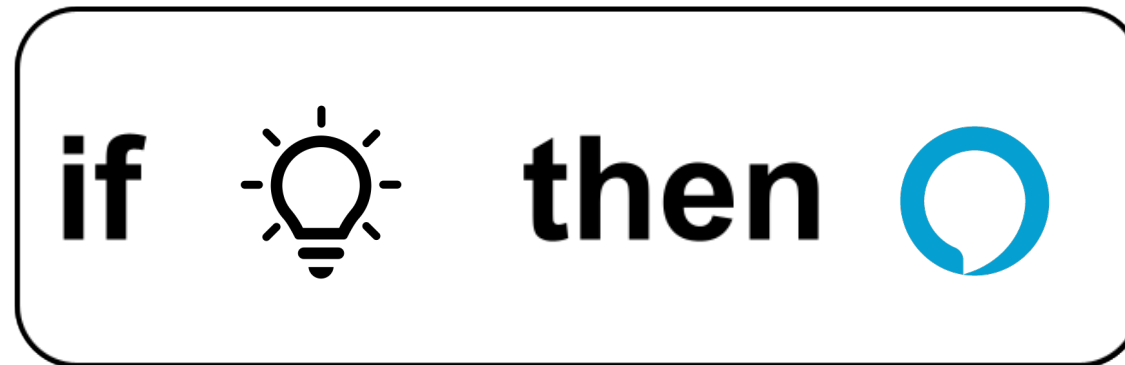





Alexa! Turn on my lights



# Automations via trigger-action programs (TAP)



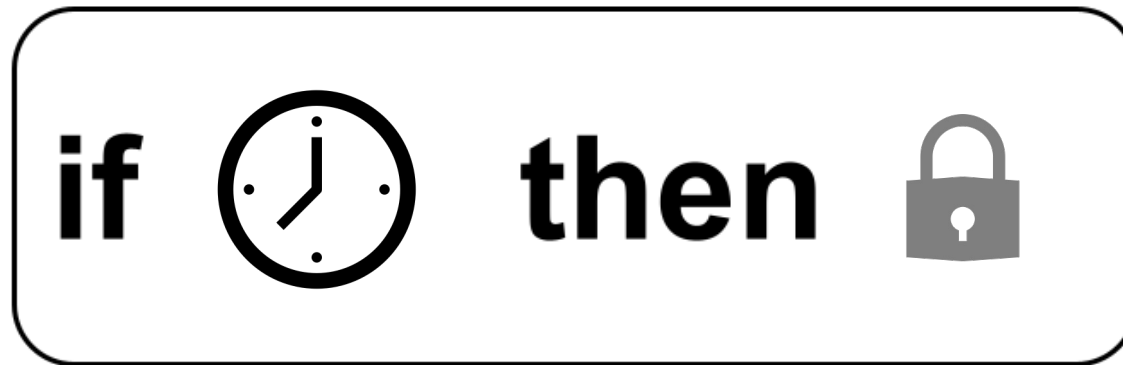
Automations can be hard to predict!

**if**  **then** 

**if**  **then** 

# Automations can be hard to predict!

[Yarosh & Zave (CHI '17)]



# Tools can identify security & privacy risks

STEP 1: PICK TEMPLATE

I always/never

\_\_\_\_\_ should

\_\_\_\_\_ and \_\_\_\_\_

should

...

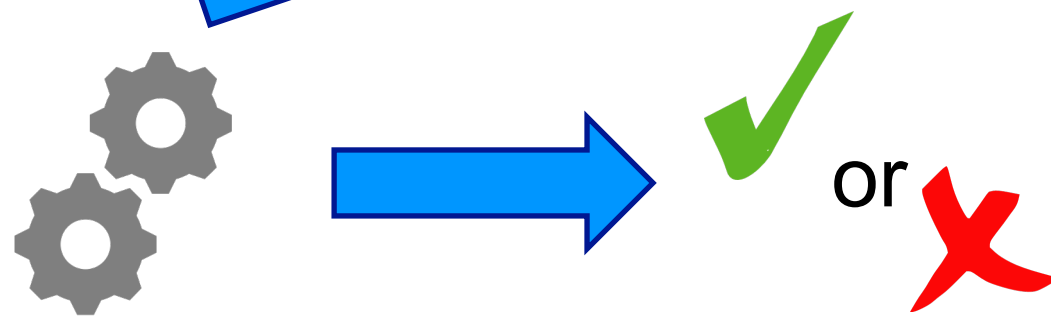
# Tools can identify security & privacy risks

## STEP 2: FILL OUT TEMPLATE

it is raining  and window open   
should  never  occur together  
 always   
 never

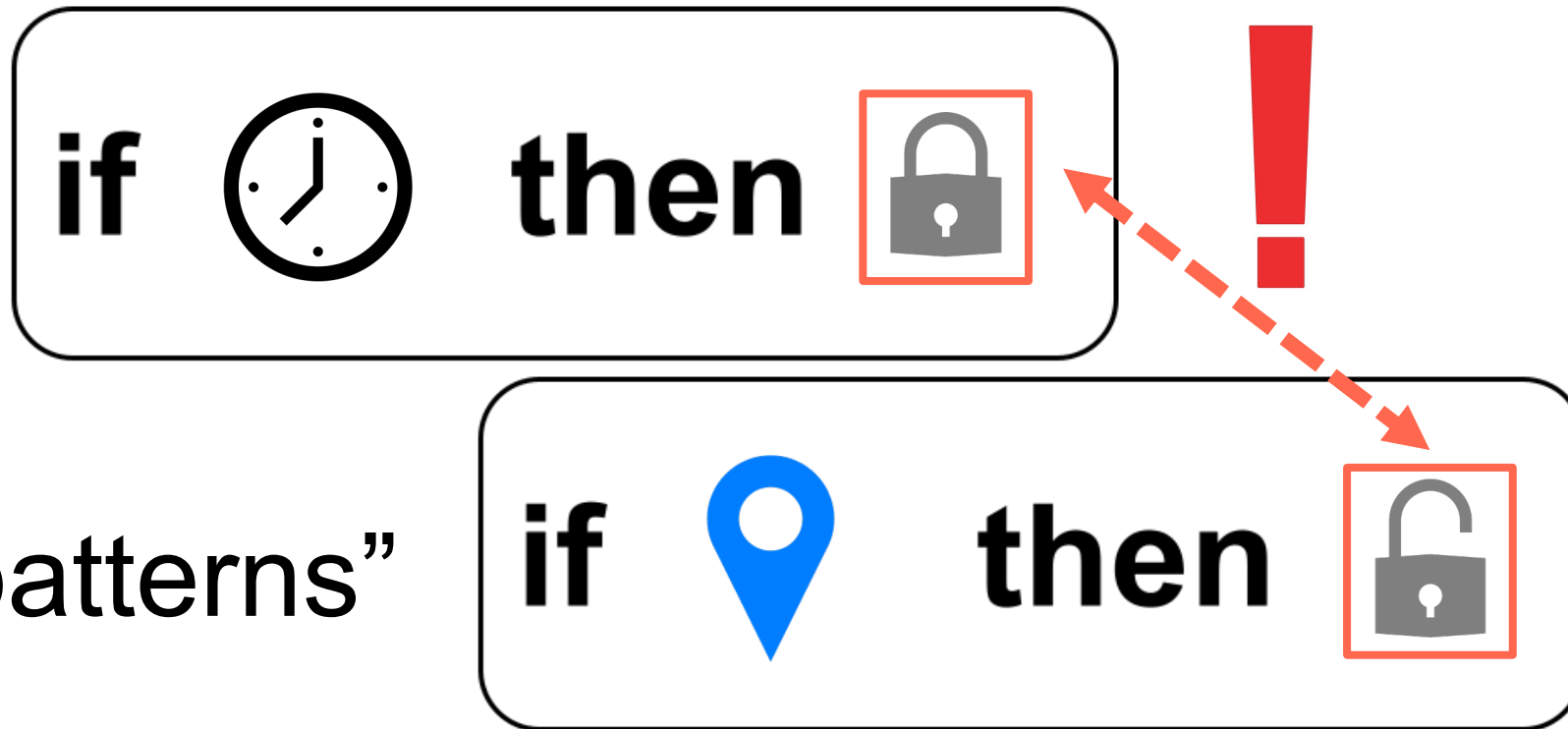
if The time then Turn off  
if A/C is on then Close window  
if Garage door is opened then Send user a notification

“Declarative Policy”

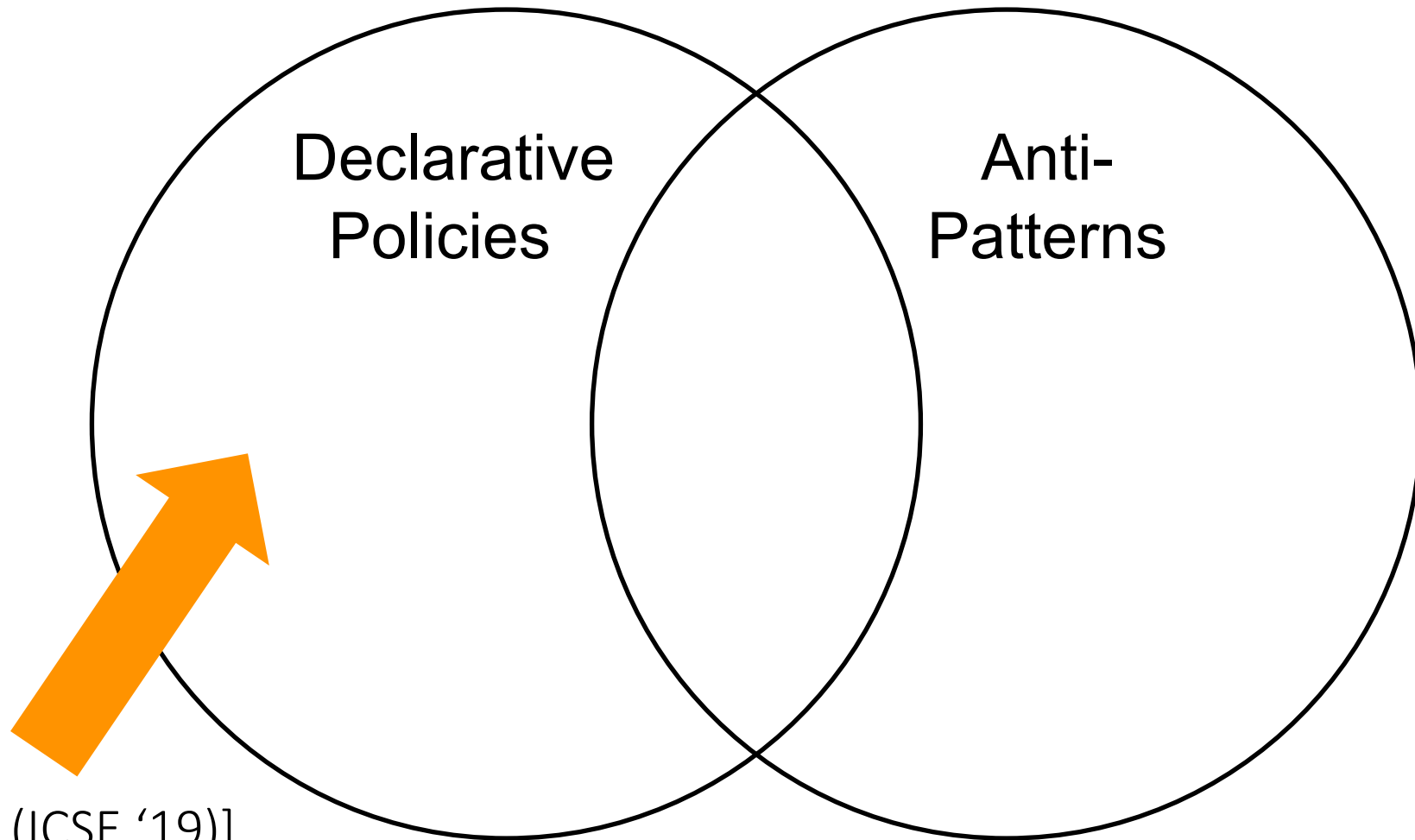




# Tools can identify security & privacy risks



“Anti-patterns”

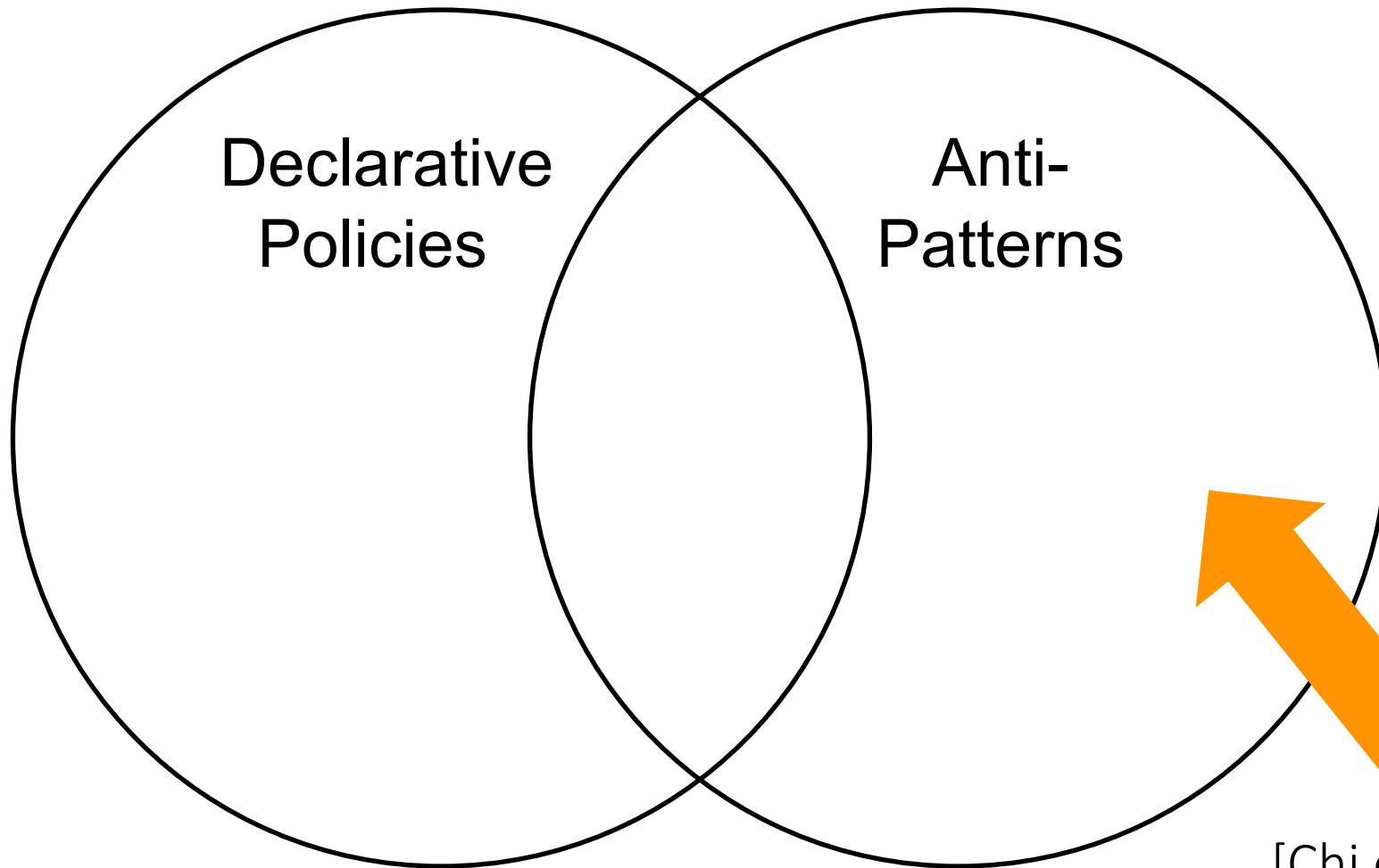


[Zhang et al. (ICSE '19)]

[Liang et al. (IPSN '15)]

[Liang et al. (BuildSys '16)]

...

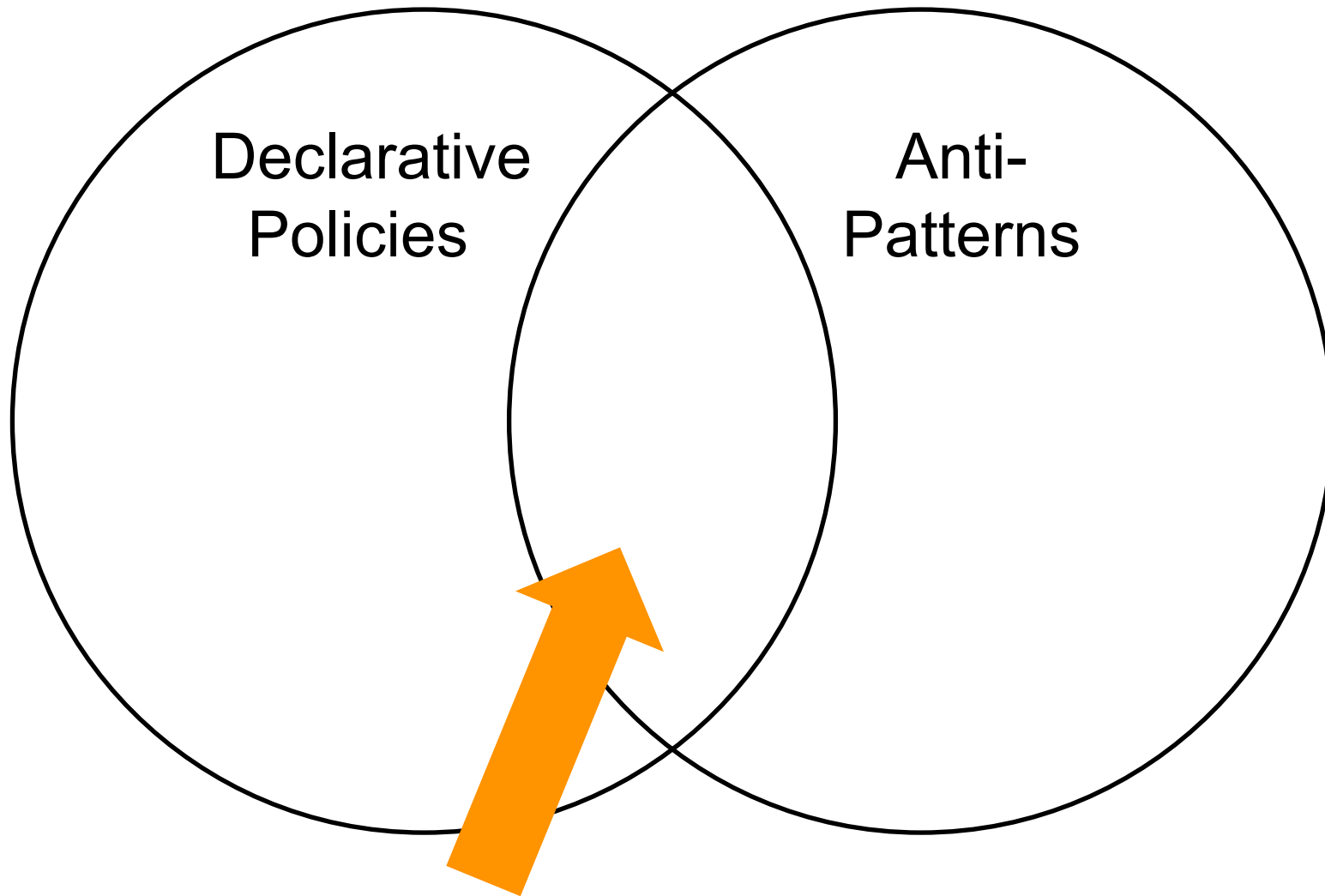


[Chi et al. (DSN '20)]

[Wang et al. (CCS '19)]

[Celik et al. (USENIX '18)]


...



[McCall et al. (2021)]

[Berkay et al. (NDSS '19)]

...



How can we make security analysis tools  
to protect smart home users  
**that can be used effectively?**

RQ 1: What **goals** do users have?

RQ 1: What **goals** do users have?

RQ 2: Can users write **declarative policies**?

RQ 1: What **goals** do users have?

RQ 2: Can users write **declarative policies**?

RQ 3: Do users understand **anti-patterns**?



RQ 1: What **goals** do users have?

RQ 2: Can users write **declarative policies**?

RQ 3: Do users understand **anti-patterns**?

RQ 4: How can tools help users  
**repair buggy programs?**



RQ 1: Goals

RQ 2: Declarative policies

RQ 3: Anti-patterns

RQ 4: Program repair

RQ 1: Goals

RQ 2: Declarative policies

RQ 3: Anti-patterns

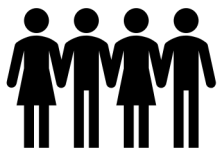
RQ 4: Program repair



Survey 1

174

Survey 2



273

RQ 1: Goals

RQ 2: Declarative policies

RQ 3: Anti-patterns

RQ 4: Program repair

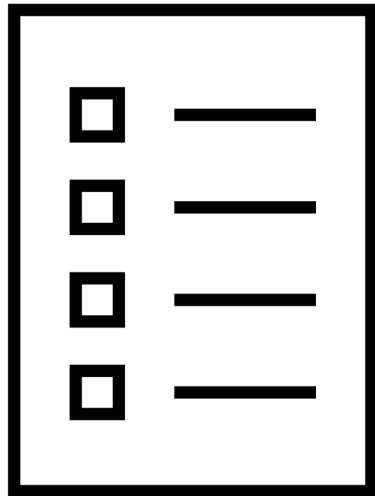
  
174

Survey 1

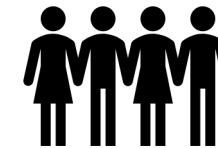
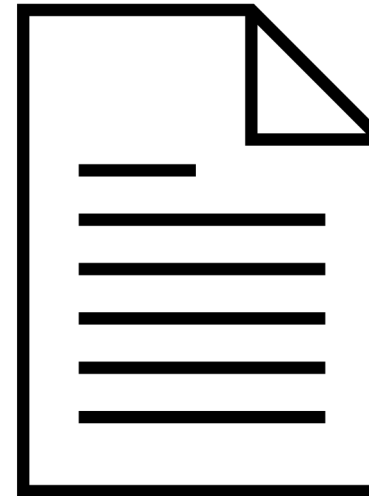
Survey 2

  
273

## RQ 1: What goals do users have?



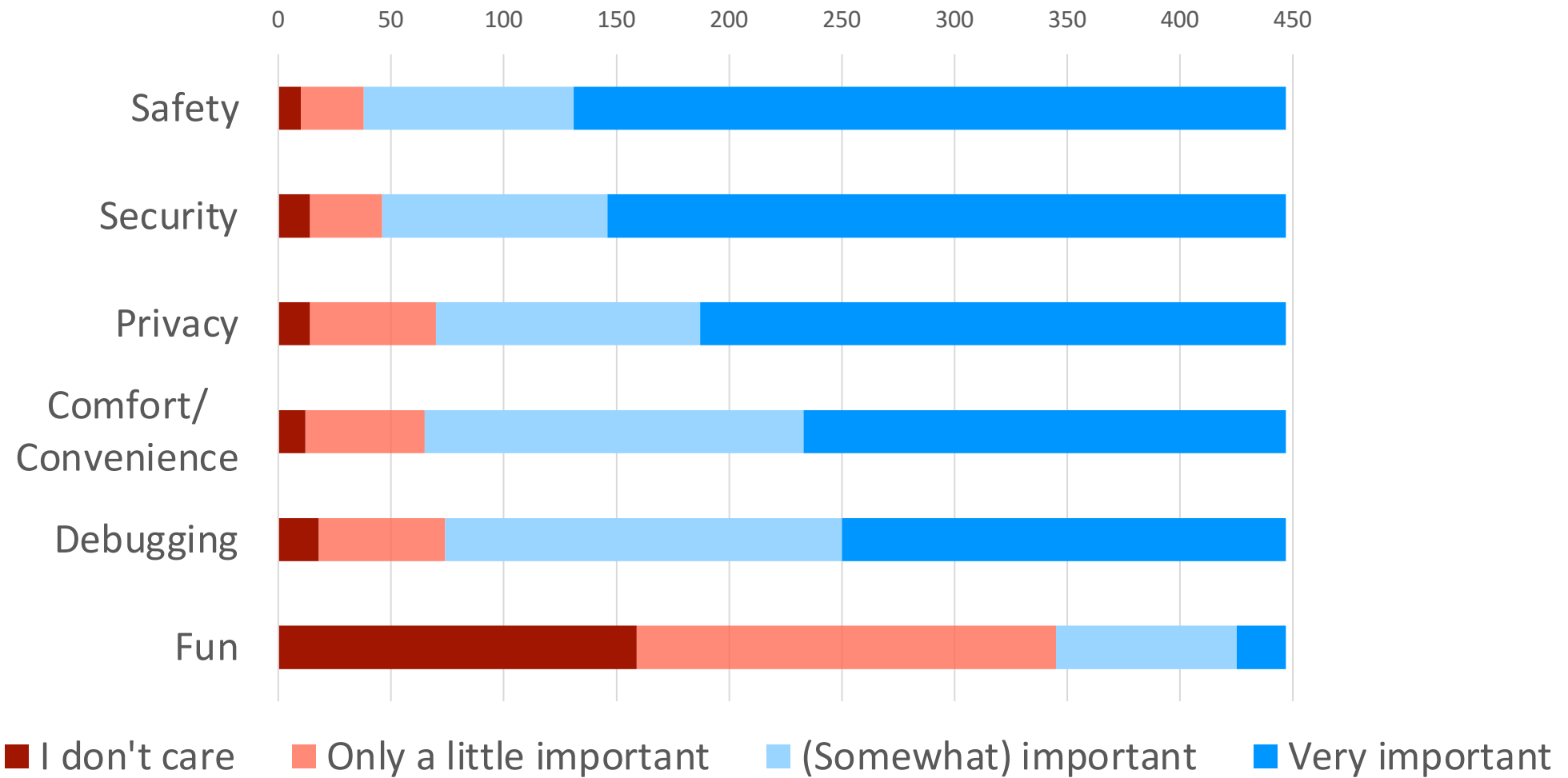
Rate the **importance** of  
**goal categories**



84%

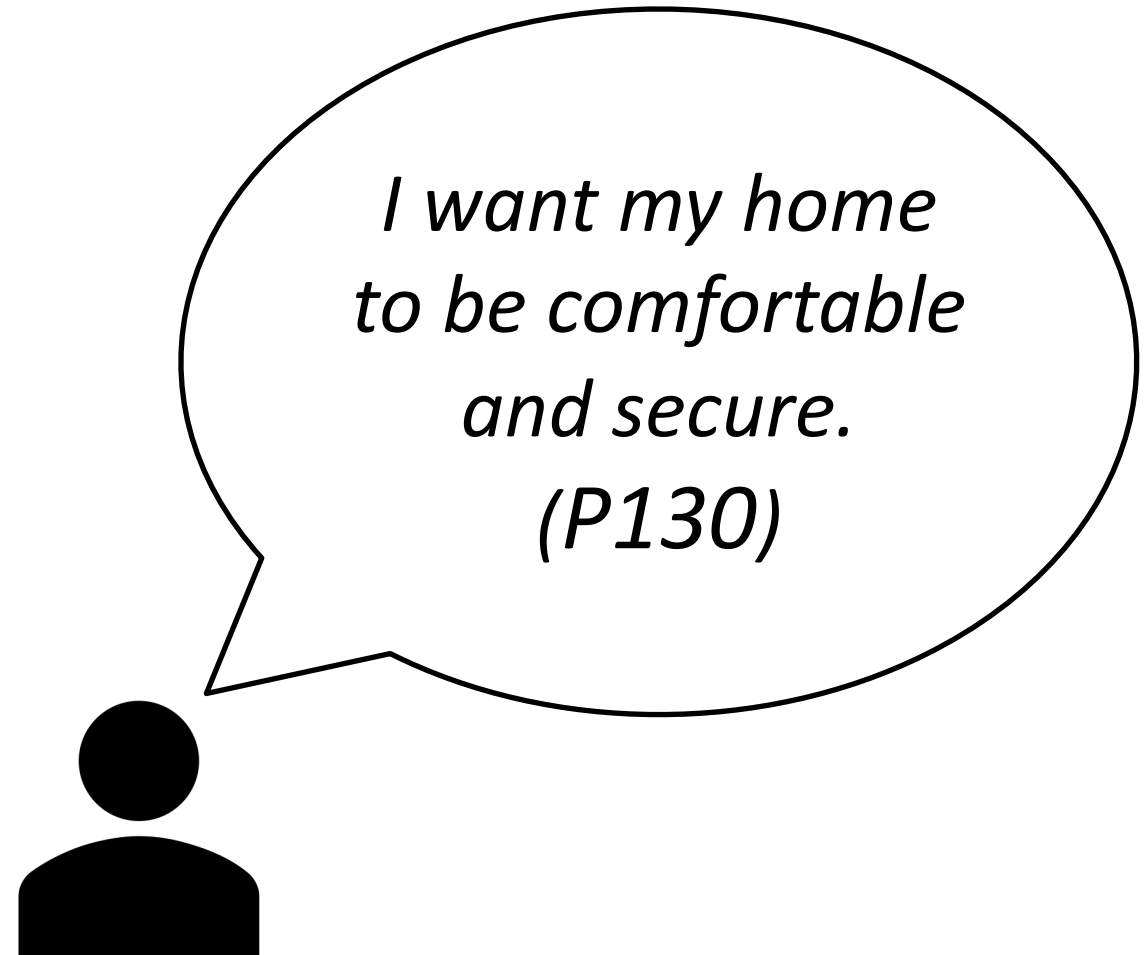
**Describe** your goals

# Everything is important! Except fun. 🍏



# How people talk about goals **varies**

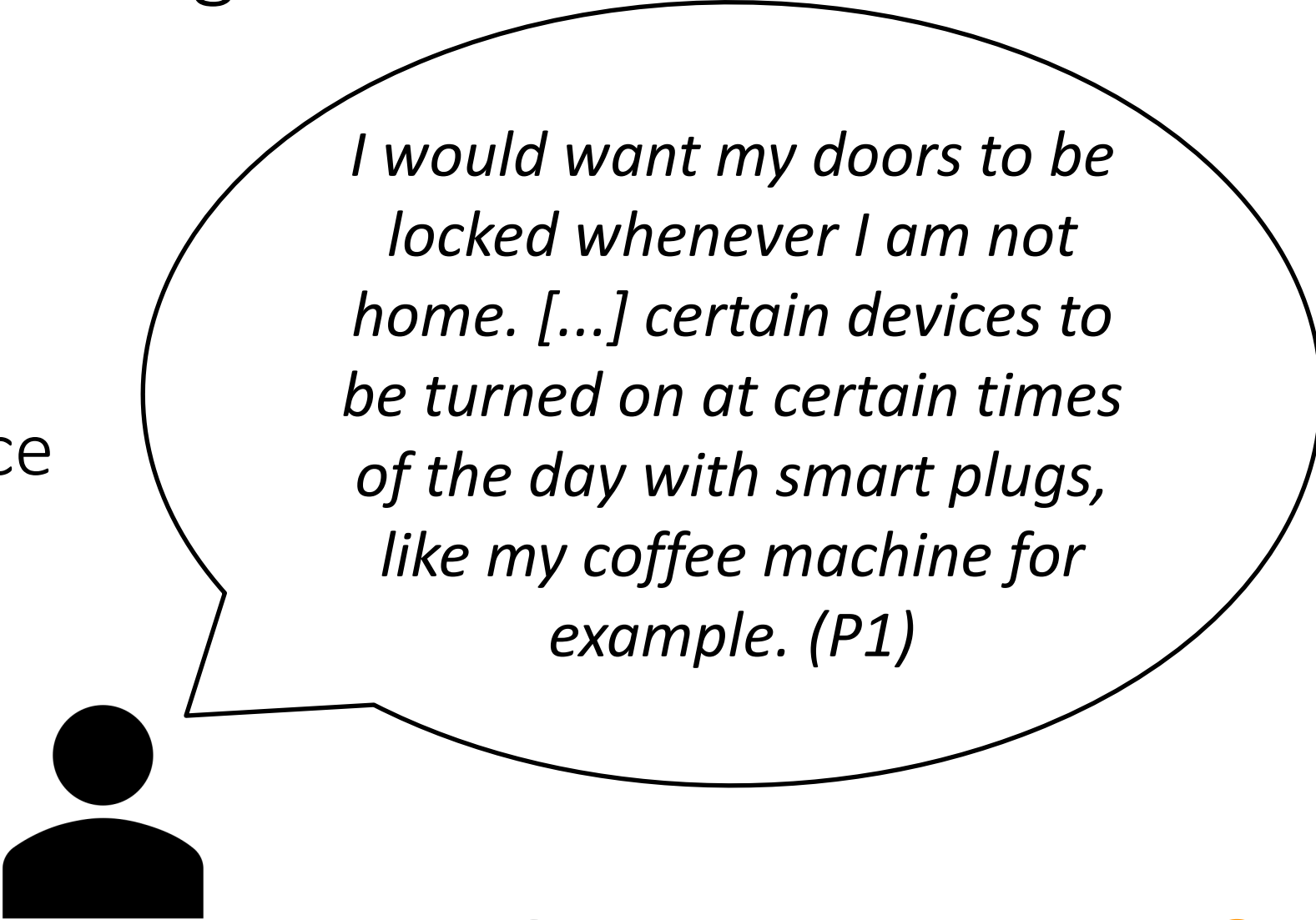
24% high-level



# How people talk about goals **varies**

24% high-level

59% specific to device



*I would want my doors to be locked whenever I am not home. [...] certain devices to be turned on at certain times of the day with smart plugs, like my coffee machine for example. (P1)*

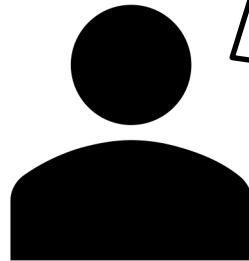


# How people talk about goals **varies**

24% high-level

59% specific to device

16% both



*My goals are to keep my home safe and secure when I leave/while I am sleeping, so I want my doors locked and secure during these situations ...  
(P113)*

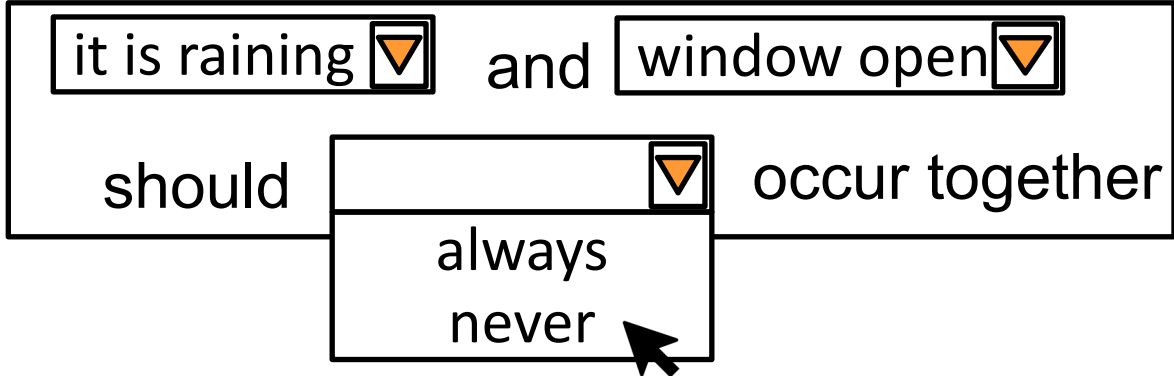
# How people talk about goals **varies**

24% high-level

59%

16%

Similar to writing declarative policies



RQ 1: What goals do users have?

RQ 2: Can users write declarative policies?

STEP 1: PICK TEMPLATE

I  
always/never  
want \_\_\_\_\_

be active while

\_\_\_\_\_ always/never  
occur together

...

STEP 2: FILL OUT TEMPLATE

it is raining

and

window open

should

always  
never

occur together

# Participants can **generally** pick policy templates

## STEP 1: PICK TEMPLATE

I  
always/never  
want \_\_\_\_\_

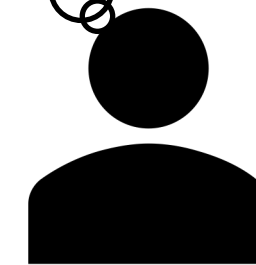
be active while

\_\_\_\_\_ always/never  
occur together

...

I want my  
lights to blink  
if there is  
smoke...

91%  
*Smoke  
detector*



# Participants can **generally** pick policy templates... **depending on the scenario**

## STEP 1: PICK TEMPLATE

I  
always/never  
want \_\_\_\_\_

be active while

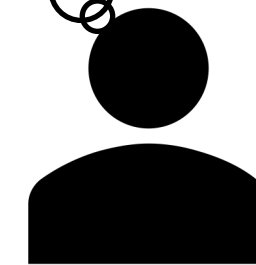
\_\_\_\_\_ always/never  
occur together

...

I don't want  
my lights to  
annoy my  
neighbors...

91%  
*Smoke  
detector*

71%  
*Neighbors*



# Participants can **sometimes** fill out policy templates

and    
should  always/never  occur together

37%

I  always/never   
want

97%



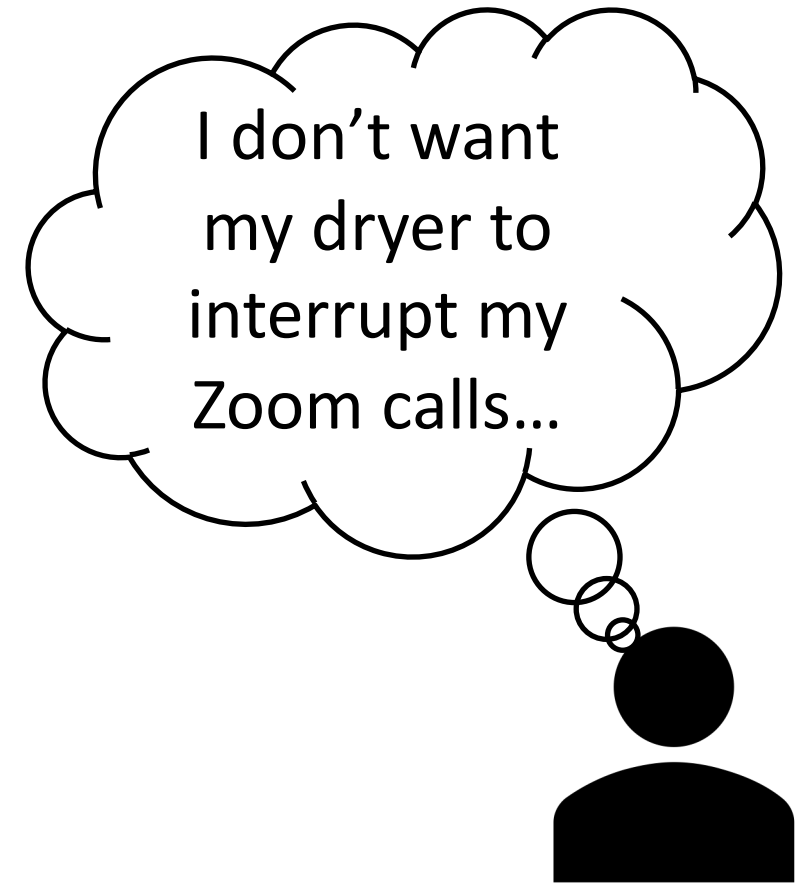
Participants can **sometimes** fill out policy templates...  
but **only sometimes**

should    
happen within    
of

12%

should    
be active while

75%



# What did we learn? What's next?

- Templates are promising!
  - Goals match policy templates
  - Success at many tasks
- ...but there is room for improvement
  - Templates should be worded carefully
  - Help understanding writing programs vs. policies
  - Examples aren't enough to understand anti-patterns



# Towards Usable Security Analysis Tools for Trigger-Action Programming

McKenna McCall, Eric Zeng, Faysal Hossain Shezan, Mitchell Yang, Lujo Bauer, Abhishek Bichhawat, Camille Cobb, Limin Jia, Yuan Tian

- Templates are promising!  
...but there is room for improvement
- Templates should be worded carefully
- Help writing programs vs. policies
- Data is available at [bit.ly/soups23-tap](https://bit.ly/soups23-tap)



*I want my home to be safe, warm, and comfortable for my family. (P14)*