Soteria: Automated IoT Safety and Security Analysis

Z. Berkay Celik

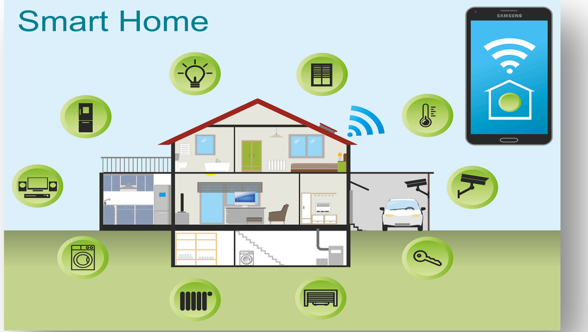
Patrick McDaniel

Gang Tan

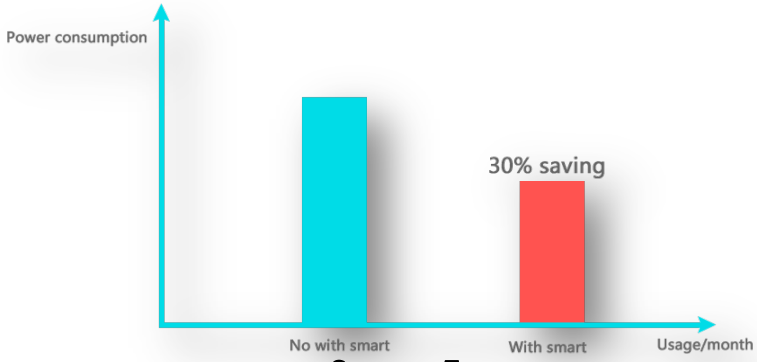
Penn State University

USENIX ATC 2018

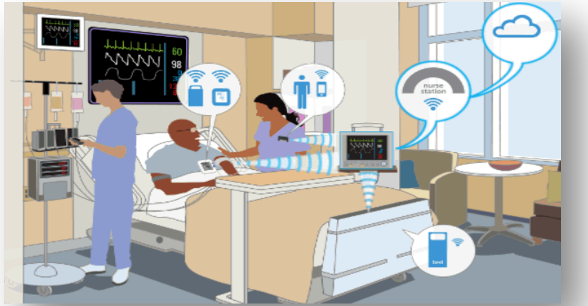
Internet of Things (IoT) enables the future



Smart Homes



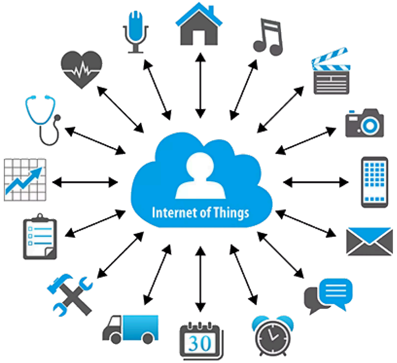
Smart Energy



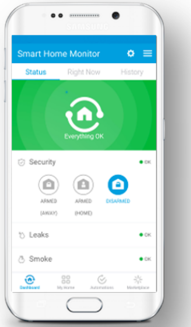
Healthcare

Smart Farms

IoT is not magic

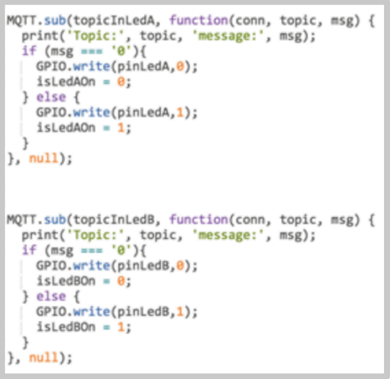


Connected devices



Mobile app

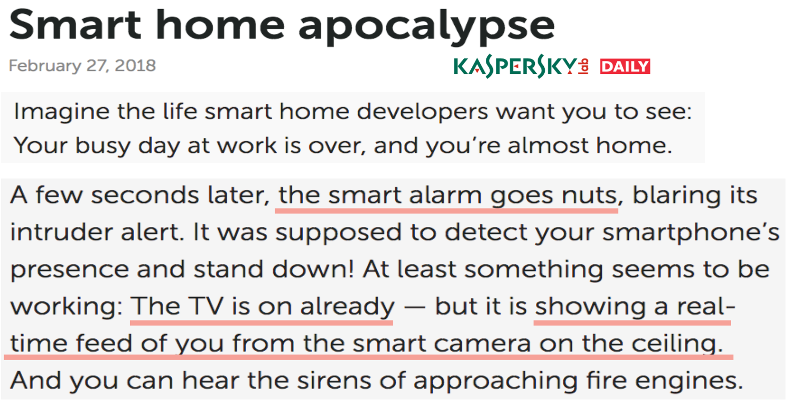
Automation



```
MQTT.sub(topicInLedA, function(conn, topic, msg) {
  print('Topic:', topic, 'message:', msg);
  if (msg === '0'){
    GPIO.write(pinLedA,0);
    isLedAOn = 0;
  } else {
    GPIO.write(pinLedA,1);
    isLedAOn = 1;
  }
}, null);


MQTT.sub(topicInLedB, function(conn, topic, msg) {
  print('Topic:', topic, 'message:', msg);
  if (msg === '0'){
    GPIO.write(pinLedB,0);
    isLedBOn = 0;
  } else {
    GPIO.write(pinLedB,1);
    isLedBOn = 1;
  }
}, null);
```

IoT application

IoT enables the future (and a whole lot of problems)

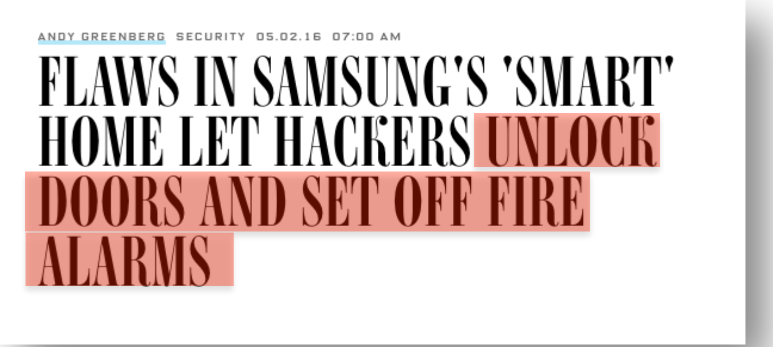


Smart home apocalypse

February 27, 2018 KASPERSKY lab DAILY

Imagine the life smart home developers want you to see: Your busy day at work is over, and you're almost home.

A few seconds later, the smart alarm goes nuts, blaring its intruder alert. It was supposed to detect your smartphone's presence and stand down! At least something seems to be working: The TV is on already — but it is showing a real-time feed of you from the smart camera on the ceiling. And you can hear the sirens of approaching fire engines.



ANDY GREENBERG SECURITY 05.02.16 07:00 AM

FLAWS IN SAMSUNG'S 'SMART' HOME LET HACKERS UNLOCK DOORS AND SET OFF FIRE ALARMS

Front door is unlocked when user is sleeping

Heater is turned on when user is not at home

Denning et al., Ronen et al., Fernandes et al., Celik et al.

In this talk…

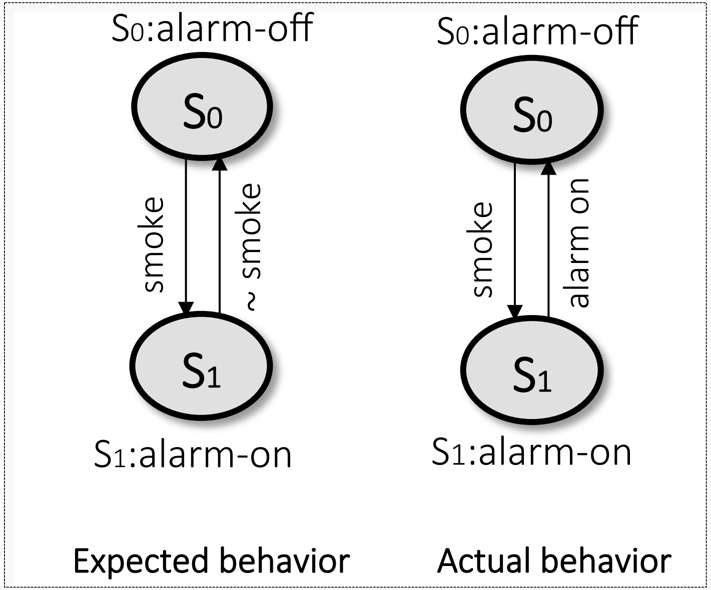
How do we ensure IoT implementations and environments adhere to safety and security properties?

Soteria*

[*] Greek goddess protecting from harm

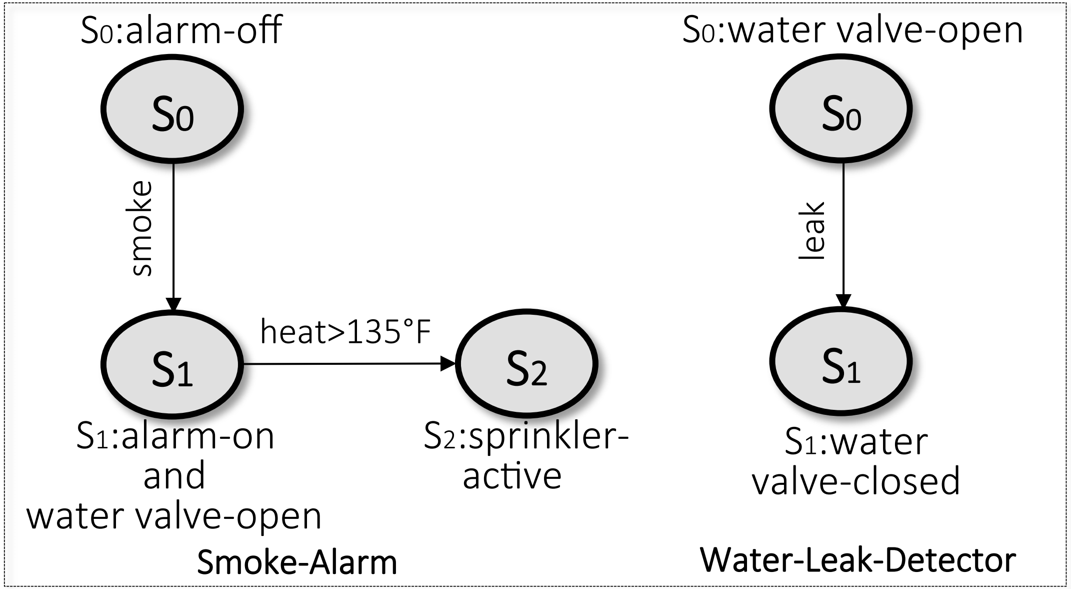
How safety/security violations happen?

Individual app



Does alarm sound when there is smoke?

IoT environment

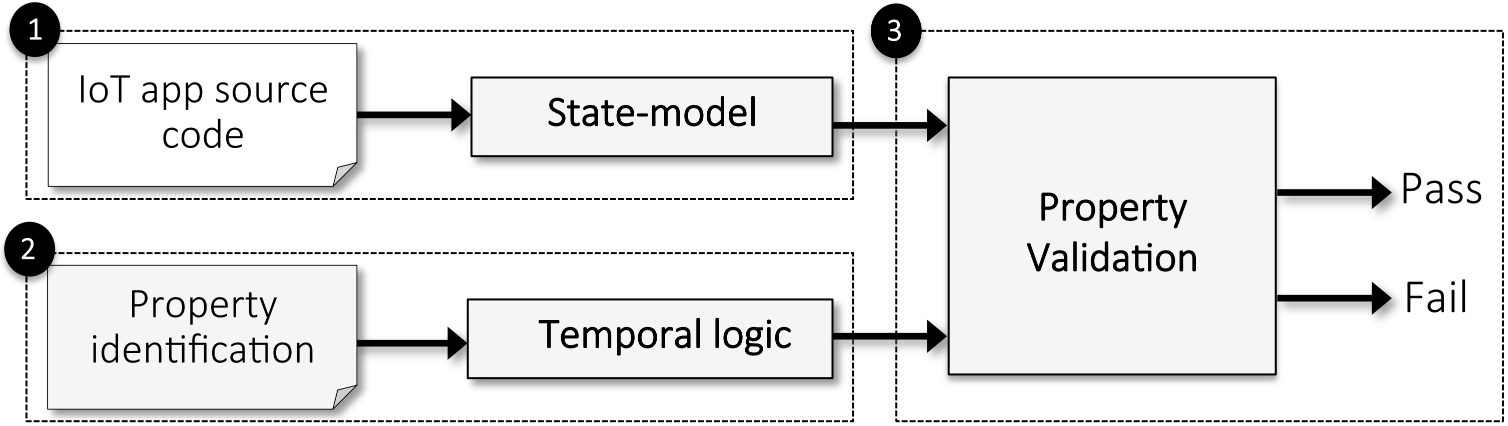


Does the sprinkler system active when there is a fire?

Soteria

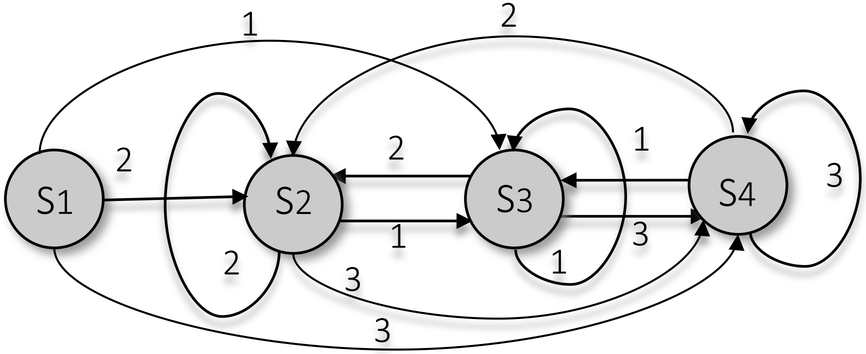
Problem: IoT platforms cannot evaluate whether an IoT app or environment (collection of apps) is safe, secure, and operates correctly

- Soteria is a static analysis system that provides formal verification by model checking of IoT apps



State-model extraction from source code

- What is state model?
  - States and transitions
  - In IoT applications…
    - **States:** Device attributes
    - **Transitions:** Events changing the attributes



State-model of an example app

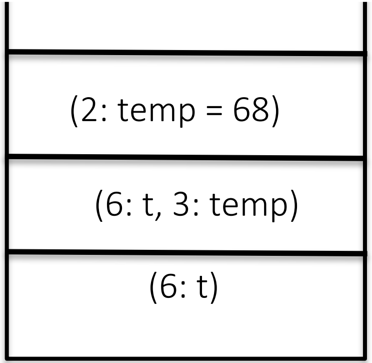
- Challenges…
  - State-explosion problem
  - Conditional device attribute changes

State reduction

- **Property Abstraction:** Reduce states by aggregating numerical-valued attributes

```
1: def modeChangeHandler(evt){
2:   def temp = 68          ❸
3:   setTemp(temp)          ❷
4: }
```

```
5: def setTemp(t){
6:   ther.setHeatingPoint(t)   ❶
7: }
```



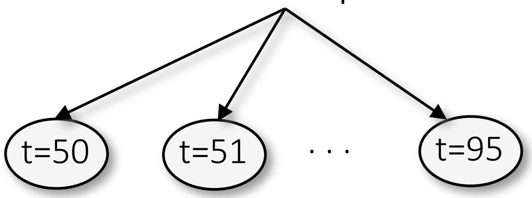
(2: temp = 68)

(6: t, 3: temp)

(6: t)

Worklist

Without property abstraction



Thermostat temperature

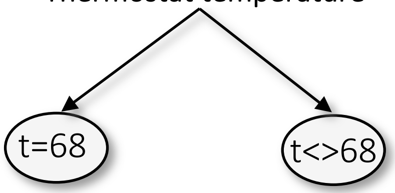
t=50

t=51

. . .

t=95

With property abstraction



Thermostat temperature

t=68

t<>68

Soteria prunes infeasible paths using path- and context- sensitivity

Conditional device attribute changes

- Perform path exploration and accumulate path conditions
  - Add a transition using end states and path conditions

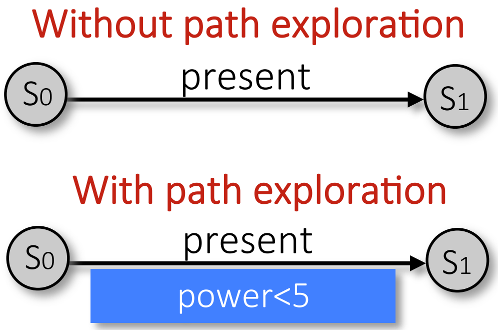
Entry point

```
subscribe(presence, present, handler)
// Entry point
handler(){
    above = 50
    below = 5
    power_val = get_power()

    if(power_val > above){
        switch.off()
    }

    if(power_val < below){
        switch.on()
    }
}
```

```
get_power(){
 latest_pow=power_meter.currentValue("power")
 return latest_pow
}
```

power>50

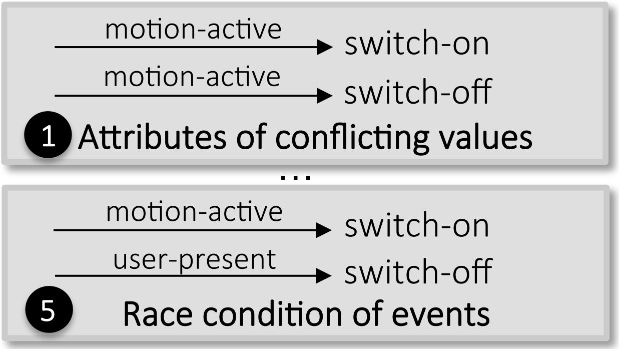
power<5



IoT safety/security property identification

- Property is a system artifact that formally expressed via temporal logic and validated on the state-model

- General properties
  - Independent of app’s semantics



$\xrightarrow{\text{motion-active}}$ switch-on

$\xrightarrow{\text{motion-active}}$ switch-off

1 Attributes of conflicting values

…

$\xrightarrow{\text{motion-active}}$ switch-on

$\xrightarrow{\text{user-present}}$ switch-off

5 Race condition of events

- App-specific properties
  - Identifies use cases of one or more devices

1 The door must always be locked when the user is not home

2 The refrigerator and security system must always be on

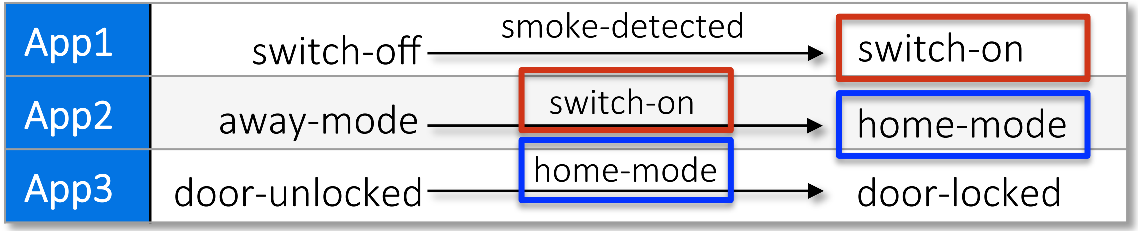
3 The water valve must be closed if a leak is detected

…

30 The alarm must always go off when there is smoke

Property validation

- Individual apps
  - **General properties are** verified at state-model extraction time
  - **App-specific properties** are validated through a model checker
- Multi-apps
  - Apps often interact through a common device
    - Create a **union state-model** of interacting apps



App1: switch-off —smoke-detected→ switch-on

App2: away-mode —switch-on→ home-mode

App3: door-unlocked —home-mode→ door-locked

❶ Is door always unlocked when there is smoke at home?

Union state-model represents the complete behavior when running the multiple apps together

Evaluation

- Implemented Soteria for SmartThings IoT platform
- Selected 65 SmartThings market apps with bias on popularity and access to various devices

Apps*	Nr.	Unique Devices	Avg/Max States
Official	35	14	36/180
Third-party	30	18	32/96

*App functionality: Safety and security, green living, convenience, home automation, and personal care

Findings - Individual app analysis

- Nine (14%) individual apps violate 10 (29%) properties

App ID	Violation Description	Violated Property
TP1	The music player is turned on when user is not at home	P.13
TP2	The door is unlocked on sunrise and locked on sunset	P.1
TP3	The location is changed to the different modes when the switch is turned off and when the motion is inactive	S.4
TP4	The flood sensor sounds alarm when there is no water	P.29
TP5	The music player turns on when the user is sleeping	P.28
TP6	The lights turn on and turn off when nobody is at home	P.13, S.1
TP7	The lights turn on and turn off when the icon of the app is tapped	S.1
TP8	The switch turns on and blinks lights when no user is present	P.12
TP9	The door is locked multiple times after it is closed	S.2

TP = Third-party

P = App-specific properties
S = General properties

Findings - Multi-app analysis

- 17 (26%) apps interacting in three groups and violate 11 (31%) properties

Gr. ID	App ID	Event/Actions	Violated Pr.
1	O3	contact sensor open → switch-on	S.1, S.2, S.3
	O4	contact sensor open → switch-off	
		contact sensor close → switch-off	
	O8, TP12	contact sensor open → switch-off	
2	O14	contact sensor open → switch-off	S.2, S.4
	O9, O16, TP3	motion active → switch-on	
	TP2	app touch → switch-on	
3	O7, TP3	switch off → change location mode	P.12, P.13, P.14, P.17, S.1, S.2
		motion inactive → switch-on	
	O30, TP21	location mode change → switch-off	
	O31, TP22	location mode change → switch-on	
	O12, TP19	location mode change → set thermostat heating	
		location mode change → set thermostat cooling	

TP = Third-party, O = Official

S = General properties
P = App-specific properties

Soteria in action…

Soteria – A system for formal verification of IoT apps through model checking

Source code

1

```
section("Turn on a pump...") {
   input ”valve_device", "capability.valve", title: "Which?",
   required: true }

def installed() {
   subscribe(valve_device, "water.wet", waterWetHandler)
}
```

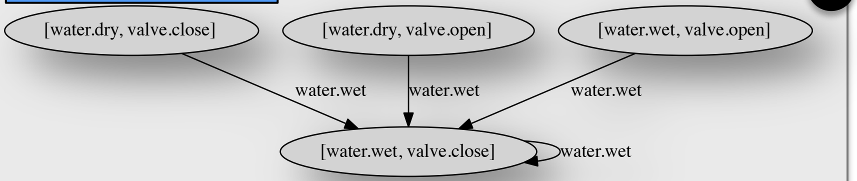
IR

2

```
// Permissions block
input (water_sensor, waterSensor, type:device)
input (valve_device, valve, type:device)
```

State-model

3



Model Checking

4

Property

SMV format of the state-model

water.wet ⇒ (AX valve.on)

Output

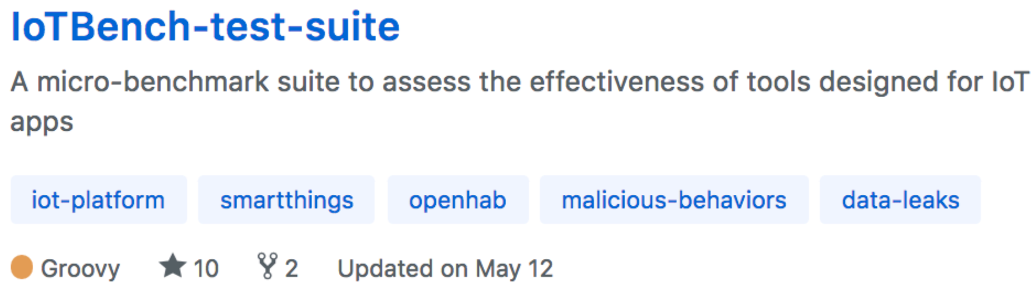
Stacktrace

5

```
Using NuSMV symbolic model checker…
General properties failed at state-model construction: none
NuSMV >> read model ...
NuSMV >> check property
NuSMV >> true
```

IoTBench

https://github.com/IoTBench/



IoTBench-test-suite

A micro-benchmark suite to assess the effectiveness of tools designed for IoT apps

iot-platform | smartthings | openhab | malicious-behaviors | data-leaks

● Groovy ★ 10 2 Updated on May 12

V.1.0.1 Released May 2018

IoTBench

27 data leaks

28 security/safety violations

15 attacks migrated from mobile phone security

500+ official and third party apps

https://beerkay.github.io

@ZBerkayCelik

berkaycelik

?

Thank you for listening!