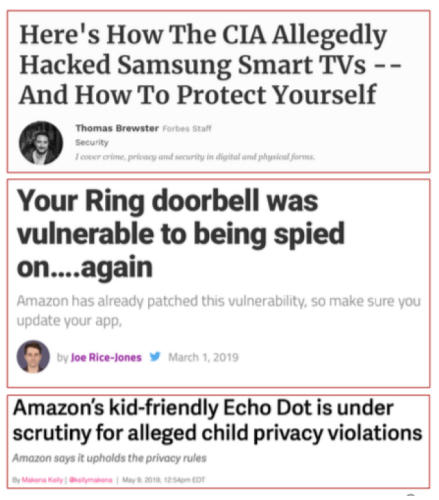
Como gravar audio subrepticiamente

- To covertly record audio from Alexa enabled devices, create a voice activated application (Alexa skill)
  - The application posed as a simple application for solving math problems but instead recorded audio indefinitely

IoT oferece pouca transparência de comportamento

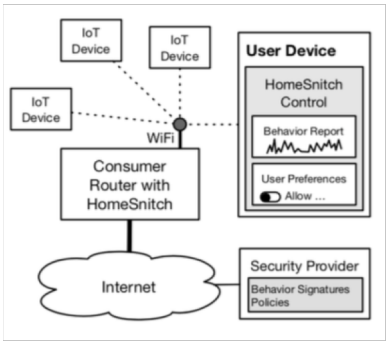
- Pode permitir a um atacante executar comportamento malicioso sem conhecimento do utilizador

How to provide transparency and control of behaviors of otherwise resource constrained smart home IoT devices?



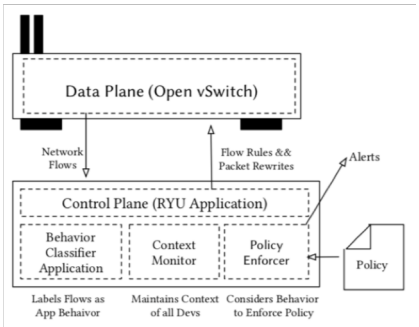
Principais desafios

- **Behavior classification**
  - Encrypted communications
  - Proprietary protocols
  - Using only transport headers
- **Network mediation**
  - Flat IP address space
  - Cannot segment the network
  - Perpetually connected devices



Abordagem

- Behavior classification
  - Classifies flows into known behaviors
  - Identifies when new behaviors occur
- Policy enforcer
  - Translates policy into network rules
  - Uses OpenFlow modifications for traffic



Comportamentos

- Classify **just based on activity alone** insufficient; devices implement activities differently
- Behaviors are a triple of **<Vendor>,<Device>,<Activity>**, examples:
  - <Ring>,<Doorbell>,<Heartbeat>
  - <Ring>,<Doorbell>,<Video>
  - <Canary>,<Security Camera>,<Video>
- Behavior triples used to find the next nearest behavior to the vendor, type of device and activity

Classificação de tráfego

Behavior: ***Nest, Protect, Alarm Test***
Protocol: HTTP-over-TLS
DPORT: 443
DST: 216.58.217.213 (Google Cloud)

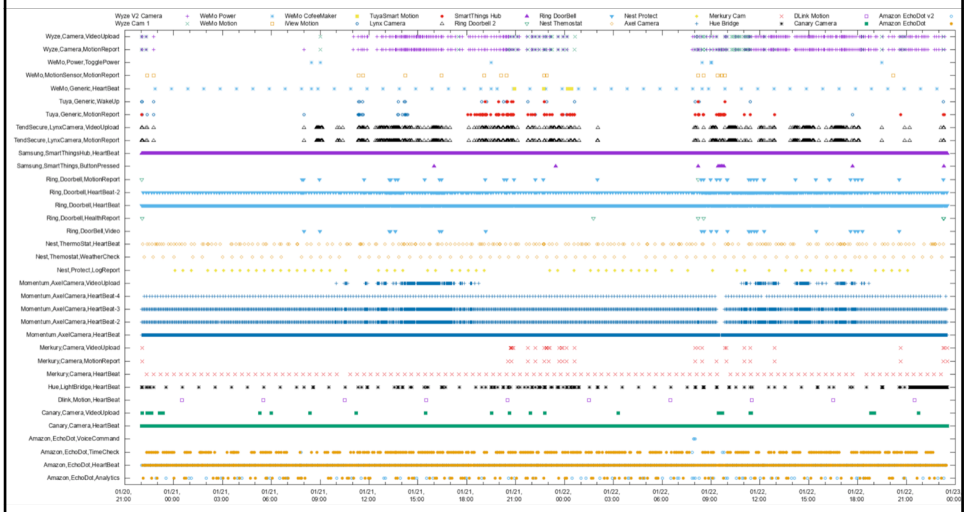
Behavior: ***Canary, Camera, Video***
Protocol: HTTP-over-TLS
DPORT: 443
DST: 52.0.14.180 (Amazon AWS)

Features para classificação de comportamento

- Throughput
- Burstiness
- Synchronicity
- Duration

Feature	Category	Importance
Avg. bytes from client per seq.	**Throughput**	**0.213104**
Avg. bytes from server per seq.	**Throughput**	**0.072519**
Aggregate server bytes sent for ADU	Throughput	0.105775
Aggregate client bytes sent fo ADU	Throughput	0.117552
Min bytes from client for single seq.	**Burstiness**	**0.038917**
Min bytes from server for single seq.	**Burstiness**	**0.038344**
Max bytes from server for single seq.	Burstiness	0.079063
Max bytes from client for single seq.	Burstiness	0.135909
Stdev of bytes for server seq.	Burstiness	0.054491
Stdev of bytes for client seq.	Burstiness	0.050798
Server sequences per ADU	Synchronicity	0.013566
Client sequences per ADU	Synchronicity	0.016211
Total time of connection	Duration	0.063750

Classificação dos comportamentos



Aplicação de políticas

ring

OFPST_FLOW reply (OF1.3) (xid=0x2):

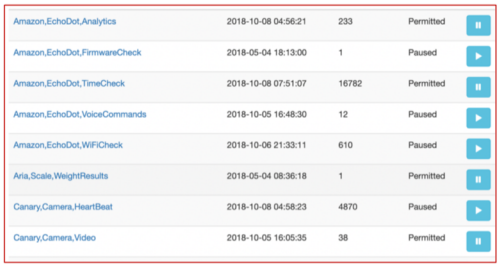
n_bytes=5488, actions=drop

n_bytes=25974, actions=drop

D-Link

OFPST_FLOW reply (OF1.3) (xid=0x2):

n_bytes=1936, actions=drop



Policy Language: Device, Behavior, Context → Action

Três problemas sérios na plataforma SmartThings

- Como impedir que as aplicações tenham **acesso abusivo aos smartdevices** dos utilizadores?
- Como impedir que as aplicações efectuem **acções sem o conhecimento** dos utilizadores?
- Como impedir que diferentes aplicações **interfiram entre si causando problemas de segurança** aos utilizadores?

Uma data de problemas

Smart home apocalypse

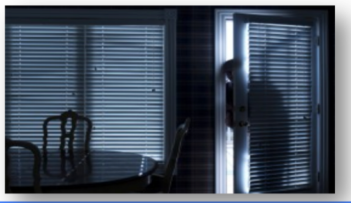
February 27, 2018 KASPERSKY DAILY

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

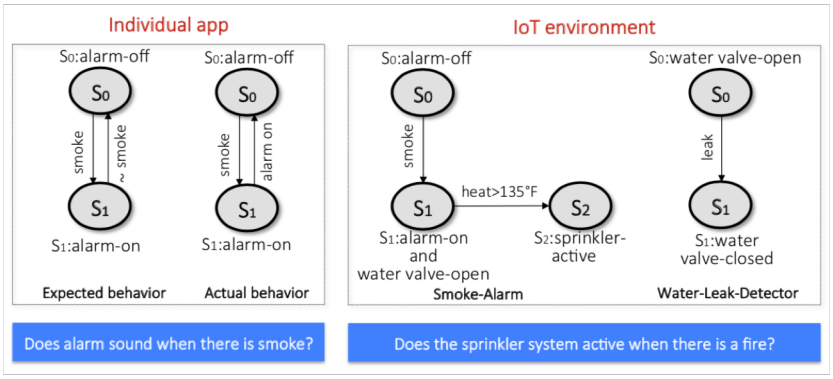
Heater is turned on when user is not at home

Nosso foco agora

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

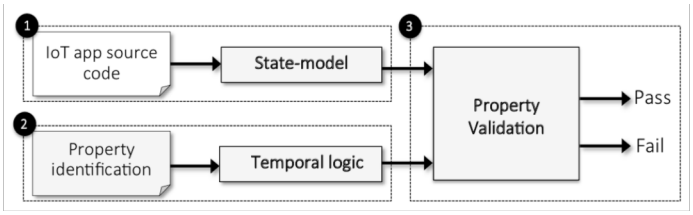
Safety: The expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.
ISO/IEC/IEEE 24765:2010 "Systems and software engineering — Vocabulary"

Exemplos de violações de segurança



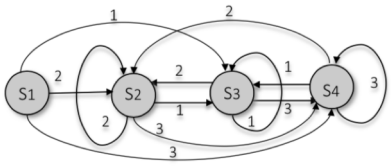
O sistema Soteria

- 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



Extracção de um modelo de estado

- What is state model?
  - States and transitions



State-model of an example app

- In IoT applications…
  - States: Device attributes
  - Transitions: Events changing the attributes
  -
- Challenges…
  - State-explosion problem
  - Conditional device attribute changes

Conditional device attribute changes

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

Entry point

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

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

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

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

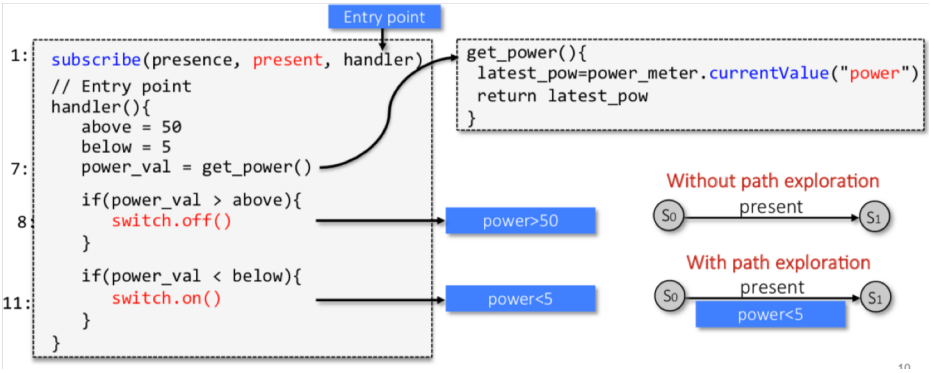
power>50

power<5

Without path exploration

With path exploration

Construção do modelo



Identificação de propriedades de segurança

- General properties
  - Independent of app's semantics

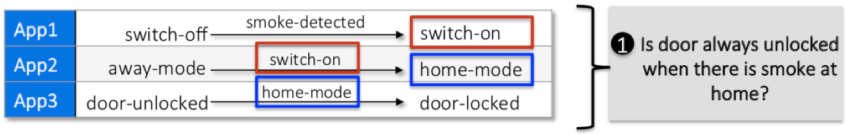
motion-active → switch-on
motion-active → switch-off
1 Attributes of conflicting values
...
motion-active → switch-on
user-present → switch-off
5 Race condition of events

- 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

Validação das propriedades

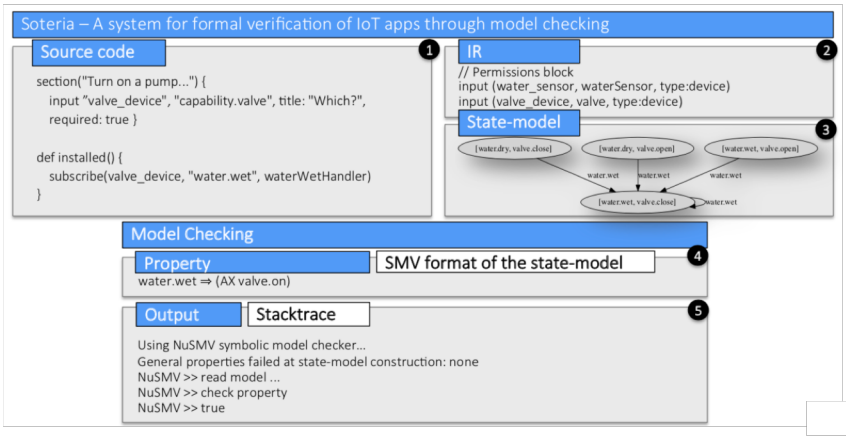
- Individual apps
  - **General properties are** verified at state-model extraction time
  - **App-specific properties** are validated through a model checker
- Multi-apps
  - Apps often interact through a common device
    - Create a **union state-model** of interacting apps



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

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

Soteria em acção



Avaliação: 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

Avaliação: 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

Conclusões

- IoT promete introduzir grande número de novas aplicações, mas também traz consigo numerosos riscos de *security* e *safety*
- Muitos desses riscos têm sido amplamente estudados e podem trazer consequências graves para os utilizadores, como demonstrado por numerosos ataques
- Em particular, a plataforma SmartThings padece de vários problemas de segurança que a comunidade de investigadores tem procurado resolver com novas soluções