

HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes Chenglong

Fu, Temple University; Qiang Zeng, University of South Carolina; Xiaojiang Du, Temple

University <https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong> This

paper is included in the Proceedings of the 30th USENIX Security Symposium. August 11-13,

2021 978-1-939133-24-3 Open access to the Proceedings of the 30th USENIX Security

Symposium is sponsored by USENIX. HAWatcher: Semantics-Aware Anomaly Detection for

Appified Smart Homes Chenglong Fu Qiang Zeng Xiaojiang Du Temple University

University of South Carolina Temple University chenglong.fu@temple.edu zeng1@cse.sc.edu

xjdu@temple.edu Abstract As IoT devices are integrated via automation and coupled with the

physical environment, anomalies in an

appified smart home, whether due to attacks or device malfunctions, may lead to severe consequences. Prior work shows

that mined correlations are refined using various techniques to make it possible for cyber-space attacks to be extended correlations

extracted from the installed smart apps.

The correlations are mapped to the physical world. As shown in Figure 1(a), the command refined correlations are used by a Shadow Execution

“close the valve” is maliciously intercepted, which

may simulate the smart home’s normal behaviors. During run-time, it can cause room flooding. Second, very often a device may

[15] could result in fires because of a false alarm. In our testbeds and test it against totally 62 different anomaly cases. broken relay (an elec-

Introduction

actions of another, which further exaggerates the impact of anomalies. As shown in Figure 1(c), a smart lock that auto-

the rapid growth of Internet of Things (IoT), smart

atically unlock upon the resident’s presence is unlocked homes gain booming popularity. As predicted by Gartner,

due to a fake event of the presence sensor, there will be more than 500 IoT devices deployed in a typical

To address these concerns, many anomaly detection systems for smart home have been proposed. By 2022 [72], IoT devices become increasingly in-

tems [30, 35, 54, 56, 60, 68, 76] utilized data mining techniques to detect anomalies. Integrated, thanks to IoT platforms such as SmartThings

profile the system’s normal behaviors and report events that deviate from the profile. HomeKit [47], and OpenHAB [55]. These platforms provide

deviate from profiles as anomalies. However, these works do not consider the interoperability among home IoT devices by different ven-

usually take event logs as inputs without fully considering the dependencies, and allow them to work according

to user-specified

each event's semantics, which actually may be acquired from automation programs (also called smartapps).

smartapps, device types, and device functionalities. The lim- USENIX Association 30th USENIX

Security Symposium

4223 itations are threefold. First, the logic of some smartapps is too complex to be mined accurately, causing false nega-

thus, they can hardly be explained and often confuse users. Third, the learning results cannot be updated quickly when

and can be refined easily to resolve conflicts with smart apps and updated conveniently when apps change. Intuitively

We propose the notion of shadow execution for smart cations, can help improve the accuracy of anomaly detection. ho-

however, it is unknown how to represent the diverse semantic information in the form of ?

We implement a prototype HAWatcher and evaluate it event logs. 2) System behavior patterns derived from smart

on four real-world testbeds. HAWatcher reaches a high apps and those mined from events logs

may conflict. It is

precision of 97.83% and a recall of 94.12%, significantly challenging to identify and resolve these conflicts. 3) When

outperforming prior approaches. smart apps change, there are no effective methods to update the system profiling acco-

The rest of the paper is organized as follows. In Section 2, To fill the gap, we present Home

Automation Watcher

we describe background about appified smart homes. In Sec- (HAWatcher), a novel anomaly detection system for app

tion 3, we survey IoT device anomalies and present the threat home automation systems. We propose a semantics-assi-

model. In Section 4, we describe three correlation channels mining method that exploits diverse semantic information

and the representation of correlations. We present the design to construct hypothetical correlations (where a correlation

details in Section 5. The evaluation is presented in Section 6. scribes how a device state or event correlates with another)

We discuss related work in Section 7, and limitations and and use event logs as evidence to

verify them. Second, as

future work in Section 8. The paper is concluded in Section 9. the correlations are explainable according to the semantic

2 Background: Appified Smart Homes they can be easily refined to resolve conflicts with

smart apps. Third, still thanks to explainability, they can be up-

IoT devices in smart homes have become increasingly integrated conveniently according to smart

app changes. The

grated via IoT platforms for rich automation. IoT integration correlations are then used by your shadow execution modu

platforms, such as SmartThings, Amazon Alexa, and Open- to simulate normal behaviors in the virtual world. The sim

HAB, support trigger-action automation programs. On these latest states are compared to those in the real world

through

platforms, despite the huge number of IoT devices, they are both contextual checking and consequential checking, and

abstracted into a small number of abstract devices.

For ex- inconsistencies during comparison are reported as anomalies.

ample, a smart light, regardless of its brand, shape, size, and We make the following contributions.

wireless technology, is abstracted into the same abstract device, light. Each abstract device has its associated events a

We propose an novel anomaly detection solution for appi-

commands. Device vendors can have their product support fied smart homes. It meets the emerging need of detect-

integration by realizing the events and commands. In anomalies caused by IoT malfunctions or attacks.

We choose SmartThings [21] as an example IoT integration platform to present our design, as SmartThings is one of the

We propose a semantics-assisted mining method, which

the leading platforms and support sophisticated automation infuses various semantic information (smart apps, con-

logic. Other integration platforms, such as Amazon Alexa, configuration, device types, installation locations) into the

has similar structures. As illustrated in Figure 2, a typical mining process. An NLP-based approach is developed

SmartThings deployment has a cloud-centric architecture of to describe device relations for generating hypothetical

four layers. On the top is the SmartThings cloud, where smart correlations. The mined correlations

are explainable, apps run and interact with abstracted capabilities. The cloud 4224 30th USENIX

Security Symposium USENIX

Association communicates with IoT devices through the network con- states. For example, the loss

of a presence-off event could be a notification layer that uses various communication techniques

leaves the door unlocked after the resident leaves home. such as WiFi, Zigbee, and ZWave. An IoT

devices can

be Command Failures. They correspond to commands issued partitioned into the cyber part and the physical part.

The by the IoT platform that fail to be executed by the target cyber part manages interfaces for humans and bridges the

of a cyber part or physical part. (1) Cyber-part

malfunction - the latter fulfills its functions in the physical world. Taking into account that cause commands to fail to execute, such

irresponsive [11]. (2) A physical-part malfunction is equivalent - Next, we describe some terms used in

Smart Things. A

ability to malfunction in a traditional (i.e., non-smart) device. A device has one or multiple capabilities, each categorized

For example, a broken electrical relay inside a smart plug is an actuator

or sensor. Each capability defines one or more

can prevent the plug from cutting off the power supply [18], attributes. For example, a smart plug device has an attribute

although from the perspective of the IoT platform, the plug has a switch and, optionally, an attribute power. Each attribute

has been turned off. The state (i.e., value) is stored on the cloud and updated due to events sent from the

IoT device. For example, the Smart- 3.2

Attack on IoT Devices Things multi-purpose sensor has a capability contact sensor,

We survey the recent work on attacks against IoT devices, whose attribute ?contact? changes from

?open? to ?closed?

and find HA Watcher has the potential to detect the following when Smart Things receive an event of ?contact closed?

five different types of attacks. the sensor. In addition, the state of an actuator's attribute is Fake Events.

They are events maliciously injected by

at- updated due to a feedback event, which is sent by the device tacker. Fake events [80] may cause severe consequences

Motivation, Goals and Threat Model

fake presence - one event can unlock the door. Fake Commands. An attacker may inject fake commands IoT devices are

Interceptions. Events can be intercepted and

dis- and then present our goals and threat model. carded by attackers. E.g., the home security system can be 3.1

IoT Device Malfunctions

muted by intercepting the window and door sensors' wireless connections to stop them from sending sensor events [6].

Events. Faulty events refer to incorrect values received from an IoT device and, at least, launch the following attacks.

(1) *spoofed by IoT devices*. They can be caused by sensor defects. *Stealthy Commands*. The attacker can control the device

Commands. They are widely discussed in

Smart- the device, it does not execute the command but sends back a response, dubbed *'poltergeists'* [6, 12, 13].

Goals and Threat Model Users frequently reported their lights were turned on during the night. We aim to

detect both IoT device malfunctions described in Section 3.1 and

attacks in Section 3.2. We clarify

that *Event Losses (or Large Delays)*. They refer to events that HA Watcher can only detect attacks that violate correlation

a large delay on status update

[8], which was evaded our detection, which is discussed in Section 8. confirmed by SmartThings [20]. Event losses may

If feedback events are not muted, it is much like a Fake Command. USENIX Association 30th

4225instance,openingadoorinevitablyinvolvesthedoor'smove- ment,whichcouldbecapturedbybothacontactse-

Activity Channel. While user activities

impose changesondevices,devicestatesalsoreflectuseractivities. Figure3:Correlationchannels. Thus,theuserac-

assume the IoT platform is not compromised. Like

devices.Forexample,aTVbeingturnedontypicallyimplies otheranomalydetectionwork[35,51,76],weassumethe

that the user is nearby,which should be captured by

the arenoorveryfewanomaliesduringtraining.Weassume

motionsensor.Whenouserreturnshome,thereshouldbe therearenomaliciousorconflictingrulesintheinstalled

consecutiveevents,suchas'presenceon'showingtheuser's smartapps;howtodetectmaliciouslogic[71]andconfl-

proximityand'contact-sensoropen'fordooropening. rules[28,34]aretwoeparateresearchproblems,andthere 4.

RepresentationofCorrelations areexistingsolutionstothem[28,71],includingourprior work[33,34].Gartnerpred-

An event reporting that the device A's attribute ? should have more than 500 IoT devices by

2022 [72]. Given the bechangedtothevalueaisdenotedas $E?(A)$

,whileastate a densedeploymentinthefuture,weexploitscenarios

whichindicatesthatthedevice $B?sattribute?has the value whereanIoTdevicehasoneormoreotherdevicesnearby$

bisdenotedas $S?(B)$.2Wedefinetwotypesofcorrelations. to interact with, and propose to

leverage them to detect b a device?s anomalous physical behaviors. We discuss the ?

Theevent-to-event(e2e)correlation.Itmeansthatone eventshouldbefollowedby(denotedas?)another.For caseof

blocks communications reporting IoT events can be

example,givenamotionsensorAandalightB,thee2e (cid:3) $E am co tit vio en(A) ?E os$

nwitch(B)(cid:4) easilydetectedduetosessiontimeoutormissingsequence correlation means the

event numbers;wethusdonotfurtherdiscussit. $Emotion(A)$

shouldbefollowedbytheevent $Eswitch(B)$. active on 4 Correlations ? The event-to-state (e2s)

correlation. It means that one event arising implies (denoted as (cid:2)) a state Devices

deployed in the same home may correlate in

the form of co-present or temporally related events [35,39,45,68]. is true. For example, (cid:3)E

hp io gw her(plug) (cid:2) S os

nwitch(heater)(cid:4) These correlations can be attributed to the execution of smart

Epower(plug) means that, when the event

arises, the state high apps [29], physical interactions [39] or users' activities [45].

Sswitch(heater) should be true. As shown in Figure 3, we investigate the causes of these

on correlations and categorize them into three channels below. For the representation of a correlation involving condi

Correlation Channels tions, its anterior event is combined with the

conditions using the ??? symbol. For example, (cid:3)EMotion?SPresence? active

present SmartAppChannel. Smartapps not only directly cause Eswitch(Light)(cid:4) means the

event EMotion, if the condition on

active correlations between triggers and actions as programmed,

SPresence is true, should be followed by Eswitch(Light) . present

on but also imply some extra correlations that should be consid- We show in Section 5 that the two types of correlations,

implies a possible correlation

worth verification, that correlate via different channels. that is, if the light is turned on, then the motions should be in the

5

HA Watcher Design and Implementation exclusively turned on by the smart app. We first introduce the workflow of a

Channel. Two devices can correlate via a

cer- tion 5.1), and then describe the major modules in HA Watcher, in a physical property. First, an actuator device (see

a physical property, which is captured by nearby Correlation Mining (Section 5.3), 3)

Correlation

Refining sensor devices observing that property. For example, a smart (Section 5.4), and 4) Anomaly Detection (Section

2 For simplicity of description, without causing confusion we sometimes call an event and generate temporally correlated

omit the device IDs and use the simplified notations E_i and S_j . a b 4226 30th USENIX Security

Symposium USENIX Association Figure 4: Architecture of HA Watcher.

Figure 5: Detecting anomalies depicted in Figure 1. 5.1

Workflow of Anomaly Detection The Anomaly Detection module runs parallel with the applied home automation.

By applying semantic analysis to the app, HAWatcher extracts a correlation (cid:3) Ewater

? detected Evalve

(cid:4). Since attackers intentionally intercept the command closed ?close the valve? towards the valve, there is no fee

the correlation. Furthermore, if Figure 6: Codesnippet of the app LightUpTheNight. closed it is a

Command Failure caused by the valve?s

cyber-part malfunction, HAWatcher can detect it the same way.

(1). It applies symbolic execution to the Intermediate Representation. In case (b), the hypothetical e2s

correlation (cid:3) E hp io gw her (cid:2)

sensation of apps and captures the configuration information, Sswitch (cid:4) is first proposed based on the physical ch

tics of each app is represented as one or more rules, each in turning-off command is sent to the plug

and executed by the form of a tuple trigger(T)-condition(C)-action(A), which its cyber part

(hence, its Switch=off), however, due to its mean that if T occurs, when C

is true, execute A. If broken relay, the plug still supplies power and thus the power

Step (2), which converts rules to correlations, is straightforward - meter reports seven times of high power usage, which violates the

forward. Assuming T is reflected by the

event E1, and E2 aforementioned correlation and triggers an alarm.

is the feedback event due to executing A, the rule above is In case (c), as the resident does not actually return home,

converted to a correlation (cid:3) E1 ? C ? E2 (cid:4). there is no event E oc po en

ntact that follows the fake event E pp rr ee ss ee nn tce .

Taking a Smart Thing official app Light Up The Night [16] This deviates from the user activity

channel correlation shown in Figure 6 as an example, the Semantic Analysis (cid:3) E pp rr ee

ss ee nn tce ? E oc po en ntact (cid:4) and is thus reported as an anomaly.

module converts it into two correlations: (cid:3) E < Il 3 lu 0 minance ? E oL

night (cid:4) and (cid:3) E > Il 5 lu 0 minance ? E oL fig fht (cid:4). Here, note that the condi- 5.2

SemanticAnalysis tion($?Illuminance < 30 ?$ or $?Illuminance > 50 ?$) and the trigger The Semantic Analysis module ex

event in each rule refers to the same attribute of the

same semantics from smart apps and their configuration, such as

device; we thus merge the trigger and the condition to derive the temperature threshold for turning on AC and which IoT

a concise representation of the trigger events. devices are bound to which app, and (2) convert the semantics. Moreover

tion(cid:3) $E?(A)?E?(B)$ (cid:4) extracted from the smart app, we fur- Semantic analysis has been

used to detect malicious or a

by the proposed hypothetical e_2 correlation(cid:3) $E?(B)$ (cid:2) $S?(A)$ (cid:4), risky smart apps as in

[41, 50, 79]. We use the method de- b a $E?(B)$

$S?(A)$ scribed in our prior work [33, 34] to extract semantics in Step which means that the event

only arises when is b a USENIX Association 30th USENIX Security Symposium

4227 true. Such hypothetical e_2 correlations are not necessarily Table 1: Part of the adjacency

table. A cell marked

with true, and have to be verified using event logs (Section 5.3). (cid:2) means the corresponding attribute in the column

Correlation Mining

relate with the one in the row head. The full table of 73×73 is in our technical report [44]. While there exist many patterns

CarbonDioxide Contact Illuminance Motion Power Presence Humidity Sound Button

Switch both good usability and high accuracy in the context of applied home automation. Supervised mining methods

more accurate but require well annotated datasets

or users' interventions. Unsupervised methods [31, 35, 60, 68] can be applied to unannotated data, but are less accurate

Acceleration (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) CarbonDioxide (cid:2) (cid:2)

(cid:2) Instead of relying on annotated datasets, we propose a Contact (cid:2) (cid:2) (cid:2)

(cid:2) (cid:2) semantic-based mining method. Semantic information in- Illuminance (cid:2)

(cid:2) (cid:2) Motion (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2)

(cid:2) includes devices' types and installation locations, which can Power (cid:2) (cid:2)

(cid:2) be obtained from home automation platforms. Based on this Presence (cid:2) (cid:2) (cid:2)

(cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2) Humidity (cid:2) (cid:2)

(cid:2) information, HA Watcher proposes hypothetical correlations Sound (cid:2) (cid:2) (cid:2)

(cid:2) (cid:2) (in addition to those 2 correlations from smart apps) cor- Button (cid:2) (cid:2)

(cid:2) responding to physical channels and user activity channels. Switch (cid:2) (cid:2) (cid:2)

(cid:2) (cid:2) (cid:2) (cid:2) (cid:2) (cid:2)

(cid:2) Each hypothetical correlation is then verified independently. For physical channel correlations, we consider

Preprocessing Event Logs

power, and air quality. To determine whether two IoT device attributes may relate via a physical property, we develop a

be incorporated into logical calculations. We thus use the relatedness between an attribute

and a

physical design a preprocessing scheme for redundancy removal and property, we use Google's pre-trained word2vec

in the list and the physical property, and use the highest score of its readings from the entire training dataset and calculate it

as the relatedness score between the physical property and mean and standard deviation. Readings that fall outside the

range $[-3\sigma, +3\sigma]$ are excluded as extreme values

ten attributes with the highest scores, which are reconsidered (i.e., the three-sigma rule [64]).

Then, we apply the Jenks

mutually correlated via that physical property. natural breaks classification algorithm [49] to the remaining This way

device's given attribute, we traverse the events

and in Table 1. As SmartThings stipulates 73 attributes [19], the remove those that do not change the state (e.g., consecutive

table is 73×73 . A cell with (cid:2) means that the attributes in its E Illuminance). Now, each two temporally adjacent events

row head and column head correlate. the same attribute of a device have opposite values. While most of the cells are auto

Hypothetical Correlation Generation

exception is the switch attribute: as all actuator devices have the switch attribute, we mark it as correlated with all other

and motion as the two special attributes that directly user activity channels with other semantic information, such as reflection

users' activities. As a user's activity may affect

all as device attributes and relations between attributes. We first the attributes, in the adjacency table we mark presence

attribute pairs; then, we fill each pair with

de- For a specific smart home, all attributes of the installed devices that have matching attributes to generate hypothetical

may correlate. Given a pair of correlated

attributes 3 Event exclusion is for training only; the anomaly detection module ? and ? in the

adjacency table, the device A with the at- does not eliminate events.

tribute?, and B with?, we generate four hypothetical 2e results 4 IJ te sn fk os rn oa nt eu -r da il mb er

nea sik os na dl g ao tari [t 3h 8m] and K-means algorithm gives the same correlations (cid:3)E

a?(A) ?E b?(B)(cid:4),(cid:3)E a? (cid:6)(A) ?E b?(B)(cid:4),(cid:3)E a?(A) ? 4228 30th USENIX

Security Symposium USENIX AssociationE b? (cid:6)(B)(cid:4),(cid:3)E a? (cid:6)(A)?E b?

(cid:6)(B)(cid:4), and four 2s ones ((cid:3)E a?(A)?S b?(B)(cid:4), 5.4

Correlation Refining (cid:3)E a? (cid:6)(A)?S b?(B)(cid:4),(cid:3)E a?(A)?S b?

(cid:6)(B)(cid:4),(cid:3)E a? (cid:6)(A)?S b?

(cid:6)(B)(cid:4), where The accepted hypothetical correlations should not be used a and a (cid:6)

(bandb(cid:6)

,resp.)arevaluesoftheattribute?(?,resp.) directlyfortworeasons.First,conditionsofsmartappsmay afternumeric-t

overlooked if they remain unchanged during

training. erateanotherighthypotheticalcorrelationswiththeevents For instance, assume there is

a smart app that, upon the ofBasanteriors. front door opening,turns on the porch light after

sunset. Moreover,weproposetocombine semanticsfromsmart If the residents always come

back home after sunset,the appswith semanticsfromtheadjacencytable.Theintuition

(cid:3)Econtact

?Eswitch(PorchLight)(cid:4)could inaccuratecorrelation behindthecombinationisthatwhenanactioncommand

open

on beacceptedbyhypothesistestingandcausefalsealarms of smartappisexecuted,itusuallyimposescertainchange

Second,whenappschange,acceptedhypothetical aconditioextractedfromasmartapp,wecreateavirtual correlati

present

correlation extracted from smart apps, and launch there- EMotion(M) arises and PS is present. Next, the virtual device

finishing process whenever smart app changes or there

are active is used, just like the corresponding real device, to generate hypothetical correlations

accepted by hypothesis testing. hypothetical correlations according to the adjacency table.

We first define the cover relation between two correlations: a correlation C covers a correlation C' if and only if

C is extracted from a set of correlations S and C' is extracted from a subset S' of S . Our current prototype only considers devices

installed in the same room for generating hypothetical correlations. smart app covers a correlation

C if and only if C is extracted from a set of correlations S and C' is extracted from a subset S' of S . While this can be relaxed by considering any two devices

passes hypothesis testing if they meet two conditions:

1) in the home, our current implementation makes a trade-off

they have the same posterior event (i.e., $E(B) = E(D)$); and between the comprehensiveness of hypothetical correlations

$E(A) \leq E(C)$ and $E(B) \leq E(D)$ (logically) implies (i.e., \Rightarrow).

If a correlation C covers a correlation C' , and the meaningfulness of the mined correlations. a correlation C covers C' , the latter is removed. In

the example mentioned above, a smart app derived the correlation (cid:3) between the open

contact? 5.3.3 Hypothesis Testing Scenario The switch(PorchLight)(cid:4) covers the

mined correlation. It is worth emphasizing that hypothetical correlations are not sunset

on (cid:3) between contact and switch(PorchLight)(cid:4) because they have the

same necessary truth. That is why we need hypothesis testing, the open on posterior event and (E oc

po en ntact? Scenario) between E oc po en

ntact; thus, the process of verifying hypothetical correlations using event logs. Given a hypothetical correlation, we tr

latter correlation is removed. to find all events that match its anterior, and take each of them 5.5

Anomaly Detection as a testing case. Then, we check whether the hypothetical correlation? posterior event or state is

constitutes a testing case for active

shadow execution engine, which subscribes to the events of the hypothetical correlation (cid:3) E aM

cto it via event? E os

n switch(Light)(cid:4). This the installed IoT devices. It keeps track of all devices? states case is counted as a success if E

and simulates a smart home's legitimate behaviors based on short duration and

after EMotion. In our implementation, $d =$

obtained correlations. active 60s, which is long enough to wait for the feedback event to

For each incoming event, the shadow execution engine arrives but not too long ago to accept an event not related to

performs the Contextual and Consequential checkings success- EMotion. Note the scheduling granularity of SmartThings

occurs in a valid context specified in 2 correlations. After checking these test cases can be considered as a se-

that, the consequential checking searches for its consequence of independent Bernoulli trials. We use the one-ta-

tial events as predicted by 2 correlations. test [42] to evaluate each hypothetical correlation's correct-

Below, we use the same example correlation (between a sensor and a light) as in Section 4.2. For a given correlation, we set the alternative hypothe-

motion sensor and a light) as in Section 4.2. When an event $EMotion(A)$ is received, the correlation succeeds with a proba-

is received, the shadow execution engine first confirms that the correlation is active than P_0 ?. Correspondingly, the null

hypothesis H_0 is that the contextual checking. It traverses all 2 correlations and the correlation

succeeds with a probability no higher than P_0 ?.

and locate those with the event EMotion(A) at their anterior. We choose the 95% fiducial probability as in common practice.

active places. Among the located ρ^2 correlations, if any of them is significant [27], which means that the

correlation can only be due to states in their posterior places that are

inconsistent with the null hypothesis if the p -value is smaller than 5%. USENIX Association 30th

USENIX Security Symposium 4229 Table 2: Numbers of rooms, devices and apps in each testbed.

Table 3: IoT devices used in the four testbeds, their abbreviation labels, attributes and deployment information. Testbed

#Rooms	#Devices	#Smartapps	Abbr.	DeviceName	Attributes	Deployment
--------	----------	------------	-------	------------	------------	------------

11	M	SmartThings	motion on wall	MotionSensor	3 1 6 7 MS Zooz4-in-1 motion, on wall	4 1 6
----	---	-------------	----------------	--------------	---------------------------------------	-------

4	Sensor	illuminance, humidity	W	SmartThings	water	
---	--------	-----------------------	---	-------------	-------	--

on bathroom floor with the real-world devices' states, an alarm is raised report-

WaterleakSensor EMotion(A) C SmartThings contact, indoors in the event

as invalid. Otherwise, the event is ContactSensor acceleration active B SmartThings button

bedside accepted and the shadow execution engine changes its simulation state to active? active? active?

L SmartThings switch

as ceiling light, lamp each accepted event (motionAturns?active?in the example), LightBulb PS

SmartThings presence in wallet the shadow execution engine performs the consequential

Arrival sensor EMotion(A) P SmartThings switch, power

to control fan, checking. It searches all 2 correlations that have active SmartPlug

computer, and lamp at their anterior places and cache these events at their posterior A Netatmo

carbonDioxide, on kitchen AirStation sound, humidity

countertop places in a waiting list. If any event in the list is not received V ThreeReality switch

to control fan within 60 seconds (consistent with d in hypothesis testing),

SmartSwitch the shadow execution engine reports an anomaly of a missing Table 4: Automation rules used in Testbed

SmartApp rules event from its derived virtual device (defined in Section 5.3.2) if the involved condition is true, and the

R1 If M1(active) when Mode(home), then P3(on) R2

If M2(active) when Mode(home), then P4(on) device is handled in the same way as that from the real device

R3 IfMS1(active),thenL1(on)andL2(on) throughcontextualandconsequentialchecking. R4

IfMS1(inactive)for15minutes,thenL1(off)andL2(off) R5 IfMS2(active),thenL3(on) R6

IfMS2(inactive)for10minutes,thenL3(off) R7 IfMS3(active),thenL4(on) 6 Evaluation R8

IfMS3(inactive)for5minutes,thenL4(off) R9

IfMS4(active),thenL5(on) WeevaluateHAWatcherwithdatasetscollectedfrom4dif- R10

IfMS4(inactive)for15minutes,thenL5(off) R11 IfB(pressed),thentoggleP3andP4 ferent

real-world testbeds as shown in Figure 7. On each R12

IfB(held),thenturnoffallLandPandMode(night) testbed,wespendthreeweekscollectingdatasetfortrain-

R13 IfB(doublepressed),turnonP3andP4andMode(home) ing and one week for testing. We

apply collected correla- R14 IfA(CO₂>950),thenP2(on) R15 IfA(CO₂>950),thenP2(off) tions to

each event from the testing datasets to evaluate R16

IfPS1andPS2(away),thenturnoffallLandPandMode(away) HAWatcher'sperformance.WecompareHAWatcher

R17

If PS1 or PS2 (present), then turn on L1, L2, and P1 and Mode(home) other anomaly detectors. Here, we mainly present

testbed, we let the resident(s) propose desired automation, presented in Appendix A.2. which is

fulfilled by us with off-the-shelf IoT devices

and smart apps from the SmartThings official repository. We then 6.1 Experimental Setup

give them sufficient time to get familiar with the installed home automation before starting data collection. While the

Deployment. The device deployment is

depicted or home activity learning researches, such as [36, 37], none of in Figure 7. We deploy 10 different types of IoT

Table 3, including their abbreviation

labels. Note these testbeds contain mainly sensor devices but very few that the ThreeReality Smart Switch (denoted as

lights and fans. The smart plug (denoted as P) can

be Next, we describe how we set up our testbeds. used to control electrical appliances with power plugs; for Testbeds

and Participants. We deploy SmartThings

sys- example, in Testbed 1, P1 and P2 are connected to a TV and tems in four homes and Table 2 lists their basic informat

Ethical Concerns and Mitigation. We obtained the IRB 4230 30th USENIX Security

Symposium USENIX

Association Figure 7: Floor plans of four test beds and device deployment layouts (the device abbreviation labels are ill

All participants are fully aware of

the bedroom door (with C3) does not have this pattern. all the installed devices and apps. We do not use any sensi-

Observation 2: The correlation C23 means that MS3's tived devices such as cameras and microphones. The sound i

as the high lumi- and personal identifiable information (PII) is removed right nance value can be caused by multiple l

is not followed by a power-high event, as the do not target any safety-sensitive devices, such as heaters.

on TV need to be further turned on manually by the residents. We notify participants of incoming testing one day ahead

Observation 4: Physical- and user activity-channel correla- anomaly cases. We also ask participants to keep their norm

tions cannot be obtained without mining, since they are not living habits and do not panic if they notice any anomalies.

included in any smart apps. On the other hand, some corre- The purpose is to avoid their behavioral bias during testing.

lations can be easily extracted from smart apps but difficult Detail of the injected anomalies are presented to participants

tomine. For example, correlations that involved delays are after the testing.

difficult to be mined accurately, but can be precisely derived from rules, such as R4, R6, R8, and R10. 6.2

Training Training Baseline Approaches. We select the Association Training HA Watcher. From Testbed 1, we generate

Rule Mining (ARM) [24] and the One-class Support

Vec- correlations from the automation rules. In addition, we generate for Machine (OCSVM) [67]

based detectors as two base- erate totally 2,398 hypothetical correlations, including 46 line

approaches. We choose OCSVM because it is

widely used correlations from the smart app channel, 544 from the used for anomaly detection and

trained with one class of physical channel, and 1,808 from the user activity channel.

input data, which is suitable for our training data containing Then, the hypothetical correlations are checked using 22,6

no or few anomalies [53]. ARM is selected because it is a events collected from the three weeks?

training phase. In well-established method for mining correlations/rules, and total, 146

correlations are accepted by hypothesis testing,

HA Watcher is also based on correlation mining, and 130 remain after refining.

On the other three test beds, the

We perform ARM [24] on the same training dataset for portion of smart app channel correlations are 32/109, 15/55,

comparison. Since ARM algorithms require transaction-form and 8/26, respectively. Table 5

lists a portion of the corre-

inputs, we segment the training dataset at places where the correlations after refining. Some correlations reveal interesting

time interval between two consecutive events is longer than facts that are confirmed by the residents.

60s (the same as the threshold used for hypothesis testing). By using the library pymining [22], we mine 221 association

rules with the confidence threshold of 0.95. Unlike our cor- active

relation mining method that covers various attributes and Econtact(C1)(cid:4), which means the event Eacceleration

active devices, rules produced by the association rule mining are Econtact(C1) be followed by .

This is because the front door

dominated by motion sensors MS3 and MS4. All the 221 rules closed (with C1) is typically closed right after being open

have either MS3 or MS4? s motion attributes in their conse- USENIX Association 30th USENIX

Security Symposium 4231 Table 5: A portion of refined correlations acquired from Testbed 1. ID

Correlation ID Correlation ID Correlation ID Correlation C1

(cid:3)Eilluminance(MS3)(cid:2)Sswitch(L4)(cid:4) C2

(cid:3)Emotion(MS1)?Eswitch(L1)(cid:4) C3 (cid:3)Epresence(PS1)?Econtact(C1)(cid:4) C4

(cid:3)Epresence(PS1)?Econtact(C1)(cid:4) low off active on present open present closed C5

(cid:3)Epresence(PS2)?Econtact(C1)(cid:4) C6 (cid:3)Epower(P2)(cid:2)Sswitch(P2)(cid:4)

C7 (cid:3)Epresence(PS2)?Emotion(MS1)(cid:4) C8

(cid:3)Ebutton(B)?Emotion(M1)(cid:4) present open high on present active pushed active C9

(cid:3)Econtact(C1)?Eacceleration(C1)(cid:4) C10 (cid:3)Eswitch(P4)?Epower(P4)(cid:4) C11

(cid:3)Eacceleration(C1)?Econtact(C1)(cid:4) C12

(cid:3)Eswitch(L4)?Eilluminance(MS3)(cid:4) open active on high active closed on high C13

(cid:3)Eswitch(L4)?Eilluminance(MS3)(cid:4) C14

(cid:3)Eswitch(L3)(cid:2)Smotion(MS2)(cid:4) C15

(cid:3)Eswitch(L3)?Eilluminance(MS2)(cid:4) C16 (cid:3)Eswitch(P2)?Epower(P2)(cid:4) off

low on active on high on high C17 (cid:3)Eacceleration(C3)?Emotion(MS3)(cid:4) C18

(cid:3)Econtact(C1)(cid:2)Smotion(MS1)(cid:4) C19

(cid:3)Eswitch(L4)(cid:2)Smotion(MS3)(cid:4) C20

(cid:3)Econtact(C1)(cid:2)Sacceleration(C1)(cid:4) active active closed active on active

closed active C21 (cid:3)Econtact(C3)(cid:2)Sacceleration(C3)(cid:4) C22

(cid:3)Emotion(MS3)?Eswitch(L4)(cid:4) C23

(cid:3)Eilluminance(MS3)(cid:2)Sswitch(L4)(cid:4) C24

(cid:3)Eilluminance(MS1)(cid:2)Sswitch(L1)(cid:4) closed active active on high on low

off C25 (cid:3)Epresence(PS1)?Emotion(MS1)(cid:4) C26

(cid:3)Emotion(MS1)(cid:2)Sswitch(P1)(cid:4) C27

(cid:3)Eacceleration(C1)(cid:2)Scontact(C1)(cid:4) C28

(cid:3)Eacceleration(C2)(cid:2)Smotion(MS2)(cid:4) present active active on active open

active active C29 (cid:3)Eswitch(L5)?Eillumiance(MS4)(cid:4) C30

(cid:3)Eswitch(P2)(cid:2)SCO2(A)(cid:4) C31 (cid:3)Eswitch(P3)(cid:2)Smotion(M1)(cid:4)

C32 (cid:3)Epower(P3)(cid:2)Sswitch(P3)(cid:4) on high on >950 on active high on C33

(cid:3)Econtact(C2)(cid:2)Smotion(MS2)(cid:4) C34 (cid:3)ECO2(A)?Eswitch(P2)(cid:4)

C35 (cid:3)ECO2(A)(cid:2)Smotion(MS2)(cid:4) C36

(cid:3)Esound(A)(cid:2)Smotion(MS2)(cid:4) open active >950 on high active high

active C37 (cid:3)Econtact(C1)(cid:2)Spresence(PS1)?Spresence(PS2)(cid:4) C38

(cid:3)Emotion(M2)?Smode?Eswitch(P4)(cid:4) open present present active home

on Table6:ImpactofDifferentTraining-PhaseDuration one-tailtest(Section5.3.3),whichhastwoimpacts.Onthe 7

Recall #offalsealarms #ofcorrelations

onehand,evenaverysmallnumberofabnormalbehaviors (days) 3 63.63% 78.69% 212 183

intheshalldatasetswillcausesometruecorrelationstobe 6 75.35% 85.78% 147 141

rejected. On the other hand, due to the small amount of data, 9 94.57% 94.12% 15 135 12 97.25%

94.12% 8 132 many false correlations are not rejected yet. (3) Starting from 15 97.83% 94.12% 4

130 the dataset of 15 days, the performance (including the num- 18 97.83% 94.12% 4

130 ber of false alarms) does not change anymore, which means 21 97.83% 94.12% 4

130 that amount of data is sufficient for the test bed. (4) Those true correlations which have been rejected in the small da

are recovered in the larger datasets. This shows the robust- event set. There are 80 rules involving lights L4 and L5, 32

ness of the design of HAWatcher. Even if very few anomalies with illuminance sensors in MS3 and MS4, and 14 with th

arised during the training phase, true correlations can survive CO2 sensor in A. Other attributes are not seen in any rules,

given sufficient training data. (5) We examine the different asevents involving them are overshadowed by those invol

set of correlations mined based on different duration and in the four aforementioned attributes. In contrast, with our

find that some false correlations remain there until

more data is available. For example, (cid:3) Ehumidity (MS3) (cid:2) Scontact (C3) (cid:4) mining method, each attri

closed correlations and has an average of 10.5 correlations.

remains until behavior that fails the correlation appears. For the OCSVM-based detector, it takes a snapshot of all

Days 11 and 12. devices' states as a frame each time a new event arises and concatenates four consecutive frames as one

6.3 Anomaly Generation for

[48]. We use the open source OCSVM implementation in sklearn [63] and the default kernel (Radial Basis Function).

To evaluate HA Watcher, we simulate 24 cases of anomalies on Testbed 1 listed in Table 7 (totally 62 cases on the four In

We follow two criteria to select anomaly

cases: of the duration of the training phase on the performance of (1) the attacks are discussed in the literature about IoT

either modify the testing event logs (collected in

the as a training dataset, and then use the first six (6) days by fourth week) or interfere with the home automation, and the

Faulty/Fake Events. We simulate them by inserting events correlations than the subsequent ones, the overall quality

of devices, such as motion sensors [17], presence sensor [14], of correlations is not high. The

reason is that we use the and contact sensors [3], as they are reportedly unreliable. 4232 30th

USENIX Security Symposium USENIX

AssociationTable7:HAWatcher?s detection performance on Tesbed1. ?#inst. ?indicates the number of instances for

Type AnomalyDescription AnomalyCreationMethod #inst. Precision Recall

CorrelationsViolated 1 falsemotion(MS1)active 50 97.77% 86.00% C26 2

falsecontact(C1)open 50 100.00% 100.00% C9 3 Faulty/Fake falseacceleration(C1)active

inserteventsintothedataset 50 97.87% 92.00% C27 4 Events falsepresence(PS1,PS2)present

50 96.15% 100.00% C3,C5,C25,C7 5 falsebutton(B)pushed 50 100.00% 100.00% C8 6

missingmotion(MS2)active 57 100.00% 92.98% C28,C35,C36,C14 7

missingmotion(MS3)active 38 100.00% 100.00% C17 8 EventLosses/

missingcontact(C1)open removeeventsfromthedataset 11 78.57% 100.00% C3,C5,C27 9

Interceptions missingpresence(PS1,PS2)present 9 77.78% 77.78% C37 10

missingilluminance(MS3)events 46 100.00% 43.47% C12,C13 11 turnonswitch(P2):fan 50

100.00% 100.00% C30 12 Ghost/Fake turnonswitch(P3):lamp togglefromtheghostsmartapp

50 100.00% 100.00% C31 13 Commands turnonswitch(L4):light 50 100.00% 100.00%

C19 14 stealthilyturnonswitch(P2):fan togglefromthehostsmartapp 50 100.00% 100.00%

C6 15 Stealthy stealthilyturnonswitch(P3):lamp and 50 100.00% 100.00% C32 16

Commands stealthilyturnonswitch(L4):light removefeedbackevents 50 100.00% 100.00%

C23 17 Command failtoturnonswitch(L1):light 9 100.00% 100.00% C2 18 Failures(cyber)/

failtoturnonswitch(L4):light 12 100.00% 100.00% C22 19 Command

failtoturnonswitch(P2):fan cutoffdevices?powersupply 10 100.00% 100.00% C34 20

Interceptions failtoturnonswitch(P4):lamp 53 100.00% 100.00% C38 21 Command

failtoturnonswitch(L1):light 9 100.00% 66.67% C24 22 Failures(physical)/

failtoturnonswitch(L4):light coverbulbswithpaper 12 100.00% 100.00% C12,C1 23 Denialof

failtoturnonswitch(P2):fan 10 100.00% 100.00% C16 24 Executions

failtoturnonswitch(P4):lamp unplugconnectedappliances 53 100.00% 100.00% C10 Avg - - -

- 97.83% 94.12% - Event Losses/Interceptions. To simulate them, we ran- 6.4

PerformanceofAnomalyDetection domlyremoveeventsofsomedevicesfromthetestingevent WefirstevaluateH

is the number of correctly detected instances

of Ghost/FakeCommandsBothsmartlightsandplugshave that case divided by the number of

alarms reporting

that been frequently reported by users for turning on/off unex- anomaly case (i.e., ratio of true anomalies to alarms), re-

smartapp, which is not is the number of correctly detected instances

of that case known by HAWatcher, and use the app randomly issue com- divided by the number of injected instances of

rate is the number of false positives

divided by the StealthyCommandsWithcompromisedsmartlights[65]

number of IoT events. and plugs[58], attackers can control them to make stealthy but hazardous actions. We simulate

Precision =

$\frac{\text{TruePositive}}{\text{TruePositive} + \text{FalsePositive}}$ the same method as ghost/fake commands but remove the feedback even

$\text{Recall} = \frac{\text{TruePositive}}{\text{TruePositive} + \text{FalseNegative}}$ Command Failures (cyber)/Command

$\text{Interceptions FalseAlarmRate} =$

FalsePositive We simulate Command Failures (cyber-part malfunctions)

All Events and Command Interceptions on smart plugs [11] and smart Detectors for Comparison. We compare the per-

check each segment against all mined rules to detect Command Failures (physical)/Denial of

Executions anomalies. For the OCSVM-based detector, as in

[48], we Command Failures (physical part malfunctions) and Denial of take a snapshot of all devices' states as a frame

Association 30th USENIX Security Symposium

4233 the benefit brought by the combination of the two, we build

missed instances should not impose hazards, as the events two variants of HAWatcher: HAWatcher (Apps Only), which

are consistent with the fact that the residents are active during - extracts correlations from smart app only, and HAWatcher

ing the time. Similarly, the 26 missed instances of Case 10 (Mining Only), which mines correlations without using app

are illuminance readings which have similar values with real readings at the time. For Case 9, two instances are missed

Results of HAWatcher. As shown in Table

7, because two residents are back home together when one of HAWatcher has an averaged detection precision of 97.83%

Below we describe some examples to illustrate how HAWatcher detects anomalies.

Comparison. (1) As shown in Figure 8, HAWatcher achieves Detecting Case 7. Residents entering/leaving the bedroom.

the best performance across all the 24 cases. (2) HAWatcher opened the door, which is installed with an acceleration sensor.

(Apps Only) merely obtains 2 correlations from smart apps, such as C3, and cause the motion-active

event of MS3. However, it can only detect anomalies, such as Command Failures, even as

motion-active events of MS3 are intercepted/lost,

(cyber)/Command Interceptions. It gets 16.67% for both the user activity and 2 correlation C17=(cid:3)Eacceleration

has the second best performance. On average, its precision active

is 88.42% and recall 88.62%, showing the effectiveness and Detecting Case 11. Ghost/Fake Commands that try to turn

off our mining approach. However, due to the on P2 are detected due to a violation of the

correlation C30=(cid:3)Eswitch(P2) (cid:2)SCO2(A)(cid:4), which

lack of knowledge of smart apps, it misses many instances is derived from the on >950

of Cases 2, 11, 12, and 20. (4) The ARM-based detector has smart app rule R14 and accepted by the hypothesis testing. a

anomaly instances for 17 of the 24 cases, as its

rules of apps, but it would be difficult, if not impossible, for pure cover very few attributes (Section 6.2). (5) OCSVM pe

turn on the plug P2 to start the connected

fan, which not fall inside the same input vector. Epower(P2) causes the event . However, Since the

feedback high False Alarm Rate. We measure the false alarm rate of Eswitch(P2) event

is intercepted by attackers, the switch of P2 on

HA Watcher using the testing event logs (collected during the Sswitch(P2) is still at the state

. Thus, the physical channel e2s

fourth week). We consider any alarm that are not due to our off correlation $C6 = (cid:3)E_{power}(P2)(cid:2)S_{switch}(P2)$

anomaly injection and cannot be categorized as any of the high

on anomaly types listed in Section 3 as false alarms. HA Watcher Detecting Case 20. Command Failures (cyber)/Com

totally 13 anomalies other than those injected

by Interceptions are detected because of violation of the smart app channel e2 correlation $C38 = (cid:3)E$

am co tit vio en(M2)?S hm oo md ee? u tis o. nA sCm lo 2n ,g Ct 1h 3e ,m C, 2s 9i ,x an(6 d)

Ca 1re 5,d bu ee cat uo sev oio fl ta ht eio ln ars go ef dc eo lar yr sel oa f- E os

nwitch(P4)(cid:4):thecommandsareinterceptedornotprocessed someeventsfromtheilluminancesensors;three(3

. to violations of correlations C20 and C21, because

of the on In contrast, HA Watcher(Mining Only) cannot learn this cor-

large delays of some events from the acceleration sensors. relation and thus misses all instances of this case.

Such anomalies are categorized as true positives due to Event Detecting Case 21. L1 accepts the

turning-on command Losses or Large Delays (Section 3.1). They should be reported and sends the

feedback event, but due to a physical-part

to users, as the large delay may confuse users and even cause failure or DoE, the light is not on. While most of the instances

undesired automation (e.g., an unlock-door command arrives of Case 21 can be detected as

violation of the correlation

late after the user has locked the door). C24=(cid:3)Eilluminance(MS1)(cid:2)Sswitch(L1)(cid:4)(since the illumin

off keeps low but the light-switch state is on), 3 instances are

two are due to violation of C4 and C5, because there is one missed, because the room has been brightened up by natural light (hence, illuminance has already been high) when the residents stayed outside the door for a while (longer than 60 seconds) before opening the front door; C11 anomaly arises.

and C18 each cause one false alarm, and the reason is that For Cases 1, 3, 6, 9, and 10, some instances are missed,

the residents left the front door open for quite a while and which should be attributed to imperfection of anomaly simulation. While it is arguable whether anomalies are due to user behavioral deviation (rather than the inability of HAWatcher). For example, seven instances of Case 1 are missed, because the fake alarms, we consider them false alarms, as they are not due to motion-active events of MS1 happened during attacks or device malfunctions. Motion (MS1) the time when there are real events of ; such

In total, HAWatcher reports four (4) false alarms from 9,756 active 4234 30th USENIX Security

Symposium USENIX

Association Figure 8: Recall and precision of HA Watcher and four other detectors for comparison purposes. events

malware, rather than IoT malfunctions. For example, Home- per day and a false alarm rate of 0.04%. In comparison, AI

Guard [33, 34] presents the first systematic categorization and OCSVM cause 722 and 1,116 false alarms, respectively.

of threats due to interference between different automation that is, 103 and 159 per day and false alarm rates 7.40% and

apps, dubbed cross-app interference (CAI) threats, such as 11.44%, respectively.

automation conflicts, chained execution, and loop triggering; it is also the first that uses SMT solver to systematically

Performance upon Smart App Changes tests such threats. It conducts symbolic execution to extract automation rules for

an appified home, it is common that users change

the smart apps, such as installing new apps and changing the

PFirewall [32] is a unique work that notices excessive IoT configuration. However, traditional mining based anomaly

device data continuously flow to IoT automation platforms. detection needs a long time to adapt

to the changes and,

It enforces data minimization, without changing IoT devices during the adaptation time, may trigger many false alarm

or platforms, to protect user privacy from platforms. Handling such changes for anomaly detection in

applied IoTSan [61] statically analyzes smart apps to

predict home has been challenging. We conduct smart app change whether the resulting

automation may violate any safety experiments to evaluate HAWatcher's performance and com-

properties.

IoTGuard[29] instrument smart apps. Before pareit with other systems, OCSVM and ARM.

an app issues a sensitive command, the action has to pass As listed in Table 8, we create five cases

of smart app

the policies defined by users. Both rely on pre-defined poli- changes, which cover changes of trigger, condition, action

cies, while HAWatcher does not. Unlike

our work, which and the whole rule. For each case, we use one day to collect

detects IoT device anomalies, HoMonit[79] is focused on the data, and then apply HAWatcher, OCSVM, and ARM to

detecting misbehaving smart apps. Given a physical event, the collected data. The results show that HAWatcher does

Orpheus[31] checks the system call trace due to the event not trigger any alarms, while OCSVM triggers many alarms

against an automaton to detect attacks; it cannot detect for all the five cases and ARM for the

changes of R8 and

anomalies such as fake events, event interceptions, etc. R10. We manually inspect the alarms and confirm that they

Many anomaly detection detectors learn normal behaviors are all false alarms caused by app changes.

of a smart home from its historical data [26, 35, 51, 54, 60, 69], ARM does not trigger false alarms for the changes of

R3, 75, 76]. For example, SMART [51] trains multiple user active - R5, and R14 because it does not

include any association

ity classifiers based on different subsets of sensor readings, rules covering the devices, such as L1 and L3, involved in the

and further trains another classifier that takes the

vector updated rules. For the OCSVM-based detector, each vector

of activity-classification results as its input to detect sensor contains four consecutive snapshots of device states. In the

failures. DICE [35] detects anomalies during state transitions E switch (L1)

by checking the context. Peeves [26] makes use of data from case of R3, for example, the missing

causes unseen on an ensemble of sensors to detect spoofed events. vectors and thus triggers false alarms. For HA Watcher

Related Work

Not only is the detection more accurate, but each detected anomaly can be interpreted as a violation of a correlation, with

which itself is explainable. Prior to our work, it is unclear how home automation, their security and

privacy issues have how a mining based approach is able to accurately learn drawn great

attention [28, 29, 34, 50, 57, 61, 73, 74, 78, 79].

complex behaviors in an appified home (e.g., Testbed 1 with Most of them are focused on detecting threats, attacks and

17 apps). HA Watcher provides an effective solution. USENIX Association 30th USENIX

Security Symposium

4235 Table 8: The number of false alarms caused by smart app changes. Original Rule Type

Rule after change HA Watcher OCSVM ARM R3 Action change

If MS1 (active), then L2 (on) and L1 (on) 0 14 0 R5 New rule

IfMS2(active)B2(click),thenL3(on)L3(toggle) 0 10 0 R8 Conditionchange

IfMS3(inactive)for515minutes,thenL4(off) 0 30 67 R10 Conditionchange

IfMS4(inactive)for1530minutes,thenL5(off) 0 17 75 R14 Triggerchange

IfA(CO₂>9501000),thenP2(on)for15minutes 0 17 0 8 LimitationsandFutureWork 9

Conclusion Whiletheevaluationresultsareverypromising,weconsider

Inanappifiedsmarthome,thereexistsrichsemanticinfor- thisworkafirststeptowardssemantics-awareanomalyde-

mation,suchassmartapps,configurations,devicetypes,and tectioninappifiedsmarthomes.HAWatcherhassomeli

installationlocations.Itisapromisingdirectiontocombine tationsthatweplantoaddress.

suchsemanticinformationwithminingforanomalydetec- tion.Wepresentedaviableandeffectiveapproachinthis U

and FalseAlarmRateinSection6.4),althoughtheyoccurrarely. evaluateditonfourreal-worldtestbedsagainstvario

Ifthis neverorrarely occurs during

training,itcan causeafalsealarm.Onepotentialsolutionistoaskforusers?

Acknowledgement feedbackwhenraisingalarms,anddeactivateorre-testcor- Wethankthereviewersfortheirinva

Smartapp execution scheduling.

<https://docs.beminedyet.Wecanannotatethecorrespondingcellsinthe-smarththings.com/en/latest/ref-docs/smart>

[2] Lights follows me, 2015.

<https://github.com/the-correlationsmayconstructattacks-that-donot-violate-any>

SmartThingsCommunity/SmartThingsPublic/tree/correlations-in-order-to-evade-detection.Thebottomlineof

master/smartapps/smarththings/light-follows-me.src. runningHAWatcheristhatitimposesextraconstraints-on-at-

Door-knocker-going-crazy,2016.

<https://community.tackers.in-test-be-1-each-attribute-is-involved-in-at-least-four-smarththings.com/t/door-knocker-g>

[4] Tons of issues with smarththings, 2016.

<https://any-of-the-correlations>.For example,given the correlation

[https://www.reddit.com/r/SmartThings/comments/cid3Elock\(frontdoor\)\(cid2\)Spresence\(cid4\)\(i.e.,the-front-door-is-present-can-only-arise-when-the-presence-sensor-is-on\),if-an-attacker-smarththings/.has-compromised-the-door-lock,a-larm-will-be-triggered-if](https://www.reddit.com/r/SmartThings/comments/cid3Elock(frontdoor)(cid2)Spresence(cid4)(i.e.,the-front-door-is-present-can-only-arise-when-the-presence-sensor-is-on),if-an-attacker-smarththings/.has-compromised-the-door-lock,a-larm-will-be-triggered-if)

present-can-only-arise-when-the-presence-sensor-is-on),if-an-attacker

smarththings/.has-compromised-the-door-lock,a-larm-will-be-triggered-if [5] When st glitches

become major safety fire hazard - the attacker unlock the door when nobody is home. arXiv, 2016.

<https://community.smarththings.com/t/SparinglyDeployedIoTDevices.SomeIoTdevicesmightwhenst-glitches>

sparingly deployed, and physical-channel correlations [43]. Among them might be very few.

A promising solution is to explore the correlations in the entire home, rather than [6]. Are the

poltergeists back?, 2017. In separate rooms, which can hopefully derive more correlations

<https://community.smarththings.com/t/october-tionsamongdevices.Moreover,itistrendthatIoTdevices>

2017-are-the-poltergeists-back-devices-randomly-are-deployed-with-increasing-density.

turning-on/101402. 4236 30th USENIX Security Symposium USENIX Association [7]

Command received but not executed, [21] Smartthings, 2019.

<https://www.smarththings.com>. 2017.

<https://community.smarththings.com/t/command-received-but-not-executed/112045>. [22]

Pymining - a collection of data mining algorithms in python, 2020.

<https://github.com/bartdag/pymining>. [8] Mobile device presence update delay, 2017.

<https://community.smarththings.com/t/> [23] Troubleshooting: Smartthings

multipurpose-mobile-device-presence-update-delay/98672. pose sensor is stuck on "open" or

"closed", 2020. <https://support.smarththings.com/hc/en-> [9] Motion sensor stuck on motion,

2017.

[us/articles/200955940-Troubleshooting-SmartThings-](https://community.smarththings.com/t/) <https://community.smarththings.com/t/>

Multipurpose-Sensor-is-stuck-on-open-or-closed-. motion-sensors-stuck-on-motion/46761. [24]

Rakesh Agrawal, Ramakrishnan Srikant, et al. Fast [10] Motion sensors losing connectivity,

2017. [algorithmsforminingassociationrules](#).

InProceedings <https://community.smarththings.com/t/smarththings->

of20thInternationalConferenceofVeryLargeDataBases motion-multi-sensors-losing-connectivity-on-a-daily-

(VLDB),volume1215,pages487?499,1994. [basis/84512](#). [25] Omar Alrawi, Chaz Lever,

Manos Antonakakis, and [11] Tplink smart wi-fi plug fail, 2017. [https://www.h3-digital.com/smarthomeblog/2017/5/](#)

Security evaluation of home- [https://www.h3-digital.com/smarthomeblog/2017/5/](#)

basediotdeployments. InProceedingsoftheIEEESym- 23/tplink-smart-wi-fi-plug-fail.

posiumonSecurityandPrivacy(S&P),2019. [12] Undesired poltergeist lighting effect,

2017. [26] Simon Birnbach, Simon Eberz, and Ivan

Martinovic. [https://community.smarthings.com/t/undesired- Peeves:Physicaleventverificationinsmarthomes](https://community.smarthings.com/t/undesired-Peeves:Physicaleventverificationinsmarthomes)

In poltergeist-lighting-effect/24132. ProceedingsoftheACMConferenceonComputer&Com- municationsSecu

What?s wrong with smarthings now?, 2017. <https://community.smarthings.com/t/> [27]

KateCalder. Statisticalinference.

NewYork:Holt,1953. whats-wrong-with-smarthings-now-poltergeist-events/ 83889. [28]

ZBerkayCelik,PatrickMcDaniel,andGangTan.

Sote- ria:Automatediotsafetyandsecurityanalysis. In2018 [14] Your hotspot is a presence

detector. [http: USENIX Annual Technical Conference \(USENIX](http://usenix.org)

ATC), [//ficara.altervista.org/?p=3744&doing_wp_cron= pages147?158,2018. 1591921359.51080203056335](http://ficara.altervista.org/?p=3744&doing_wp_cron=1591921359.51080203056335)

Z Berkay Celik,Gang Tan,and Patrick D McDaniel. [15] It?s too cold, 2018.

[https://github.com/Iotguard:Dynamicenforcementofsecurityandsafety](https://github.com/Iotguard/Dynamicenforcementofsecurityandsafety) SmartThingsCommunity/SmartThings

InNetworkandDistributed master/smartapps/smartthings/its-too-cold.src. SystemSecuritySymposium(NDSS),

Light up the night, 2018. <https://github.com/> [30]

VarunChandola,ArindamBanerjee,andVipinKumar. infinitywings/SmartThingsPublic/blob/master/ Anomaly

ACMcomputingsurveys smartapps/smartthings/light-up-the-night.src/ (CSUR),41(3):15,2009. light-up-the-n

LongCheng,KeTian,andDanfengDaphneYao. Or- [17] Motion detection false positive,

2018. pheus:Enforcingcyber-physicalexecutionsemantics <https://community.smartthings.com/t/> to

defend against data-oriented attacks. In

Proceed- motion-detection-false-positive/119816. ingsofthe33rdAnnualComputerSecurityApplications [18]

Smart plug clicks but no power, 2018.

Conference(ACSAC),pages315?326,2017. <https://community.smartthings.com/t/> [32]

HaotianChi,QiangZeng,XiaojiangDu,andLannan smart-plug-clicks-but-no-power/115252. Luo.

PFirewall: Semantics-aware customizable data [19] Smartthings capabilities, 2018.

<https://smarthings.com/docs/api-ref/capabilities>. flow control for home automation systems.

arXiv developer.samsung.com/docs/api-ref/capabilities.

preprint arXiv:1910.07987, 2019. html. [33] Haotian Chi, Qiang Zeng, Xiaojiang

Du, and Jiaping [20] Known mobile presence issues and faq, 2019. Yu. Cross-app interference

threats in smart homes: <https://support.smarthings.com/hc/en-us/articles/>

Categorization, detection and handling.

arXiv, pages 204744424-Known-mobile-presence-issues-and-FAQ.

arXiv?1808, 2018. USENIX Association 30th USENIX Security Symposium 4237 [34] Haotian

Chi, Qiang Zeng, Xiaojiang Du, and Jiaping Zhang, and Patrick Tague. Do you feel what I hear? Yu.

Cross-app interference threats in smart homes:

enabling autonomous IoT device pairing using different Categorization, detection and handling. In

50th An- sensor types.

In 2018 IEEE Symposium on Security and Privacy and 2018 IEEE/IFIP International Conference on Dependable

Privacy(S&P),pages836?852,2018. SystemsandNetworks(DSN),pages411?423,2020. [46]

TimothyWHnat,VijaySrinivasan, JiakangLu, TamimI [35]

JiwonChoi,HayoungJeoung,JihunKim,YoungjooKo,

Sookoor,RaymondDawson,JohnStankovic,andKamin WonupJung,HanJunKim,andJongKim.Detectingand

Whitehouse.

Thehitchhiker?sguidetosuccessfulresi- identifyingfaultyiotdevicesinsmarthomewithcon-

dentialsensingdeployments. InProceedingsofthe9th textextraction.

In48thIEEE/IFIPInternationalConfer-

ACMConferenceonEmbeddedNetworkedSensorSystems enceonDependableSystemsandNetworks(DSN),201

(SenSys),pages232?245,2011. [36] DianeJCook,AaronSCrandall,BrianLThomas,and [47]

Apple Homekit. Homekit-apple developer, 2019. NarayananCKrishnan.

Casas:Asmarthomeinabox.

<https://www.apple.com/ios/home/>. Computer,46(7):62?69,2013. [48] Jun Inoue, Yoriyuki

Yamagata, Yuqi Chen, Christo- [37] Diane J Cook, Michael Youngblood, Edwin O Heier-

pher M Poskitt, and Jun Sun. Anomaly detection for a man, Karthik Gopalratnam, Sira Rao,

Andrey Litvin, water treatment system using unsupervised machine and Farhan Khawaja.

Mavhome: An agent-based smart learning. In 2017 IEEE International Conference on Data Mining.

In Proceedings of the First IEEE International Con-

Mining Workshops (ICDMW), pages 1058-1065, 2017. ference on Pervasive Computing and Communications (P

[49] George F Jenks. The data model concept in statistical mapping.

International yearbook of cartography, 7:186- [38] Borden Dent.

Cartography? thematic map design. 1999. 190, 1967. pages 147-149. [50]

Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rah- [39] Wenbo Ding and Hongxin Hu. On

the safety of

IoT. In Proceedings of the 2017 ACM SIGSAC conference on computer systems, pages 1-12, 2017.

In Proceedings of and Shanghai Jiao Tong University.

Contextiot: Towards the 2018 ACM SIGSAC Conference on Computer & Communications Security - providing contextual integrity to applications

Nancy El Hady and Julien Provost.

A systematic survey on sensor failure detection and fault-tolerance in [51] Krasimira Kapitanova,

Enamul Hoque, John A. Ambient assisted living. *Sensors*, 18(7):1991, 2018. Stankovic, Kamin

Whitehouse, and Sang H Son. Being smart about failures: assessing repairs in smart [41]

Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. homes.

In Proceedings of the 2012 ACM Conference on Security analysis of emerging smart home applications. Ubiquitous

Stylianos P. Kavalakis and Emmanouil Serreilis. Security [42] Ronald Aylmer Fisher.

Statistical methods for research issues of contemporary multimedia implementations: workers. In

Breakthroughs in statistics, pages 66-70. The case of sonos and sonosnet.

In The International Springer, 1992.

Conference in Information Security and Digital Forensics (ISDF), pages 63-74, 2014. [43] Milan

Fránik and Miloš Čermák. Serious flaws found in multiple smart home [53]

Shehroz SKhan and Michael GMadden. One-class hubs: Is your device among them?,

2020.

sification: taxonomy of study and review of techniques. <https://www.welivesecurity.com/2020/04/22/serious->

The Knowledge Engineering Review, 29(3):345-374, 2014. flaws-smart-home-hubs-is-your-device-among- [54]

Palanivel AKodeswaran, Ravi Kokku, Sayandeep Sen, them/. and Mudhakar Srivatsa. Idea: A

system for efficient [44] Chenglong Fu, Qiang Zeng, and Xiaojiang Du.

failure management in smart IoT environments. In Pro- Hawatcher: Semantics-aware anomaly

detection proceedings of the 14th Annual International Conference for applied smart homes

(technical report), 2020.

on Mobile Systems, Applications, and Services (MobiSys), <https://github.com/infinitywings/HAWatcher.git>.

pages 43-56, 2016. [45] Jun Han, Albert Jin Chung, Manal Kumar Sinha, Mad- [55] K Kreuzer.

Openhab-empowering the smart home, humitha Harishankar, Shijia Pan, Hae Young Noh, Pei

2013. 4238 30th USENIX Security Symposium USENIX Association [56] Wenke Lee,

Salvatore J Stolfo, and Kui W Mok. A [67]

Bernhard Schölkopf, John C Platt, John Shawe-Taylor, data mining framework for building

intrusion detection- Alex J Smola, and Robert C Williamson. Estimating tion models.

In Proceedings of the IEEE Symposium on the support of a high-dimensional distribution.

Neural Security and Privacy (S&P), pages 120-132, 1999.

computation, 13(7):1443-1471, 2001. [57] Xiaopeng Li, Qiang Zeng, Lannan Luo, and Tongbo Luo.

[68]

Amit Kumar Sikder, Hidayet Aksu, and A Selcuk Ulu- T2Pair: Secure and Usable Pairing for Heterogeneous

agac. 6th sense: A context-aware sensor-based attack IoT Devices.

In Proceedings of the ACM Conference on detector for smart devices. In 26th USENIX

Security Computer & Communications Security (CCS), 2020.

Symposium (USENIX Security), pages 397-414, 2017. [69] Amit Kumar Sikder, Leonardo

Babun, Hidayet Aksu, [58] Haoyu Liu, Tom Spink, and Paul Patras.

Uncovering and ASelcukUluagac.

Aegis: a context-aware security security vulnerabilities in the belkin wemo homeau- framework for smart homes system

In Proceedings of the 2011 ACM conference on tomation ecosystem.

In 2019 IEEE International Conference on the 35th Annual Computer Security Applications Conference on Pervasive Computing

Vijay Sivaraman, Dominic Chan, Dylan Earl, and [59]

Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg S Corrobb, and Roksana Boreli.

Smart-phones attacking smart-homes. rado, and Jeff Dean. Distributed representations

of In Proceedings of the 9th ACM Conference on Security & Privacy in Mobile Systems and their

compositionality. In Privacy in Wireless and Mobile Networks (WiSec), pages Advances in

neural information processing systems 195?200, 2016. (NeurIPS), pages 3111?3119, 2013. [71]

Yuan Tian, Nan Zhang, Yueh-Hsun Lin, Xiao Feng Wang, [60] Sirajum Munir and John A

Stankovic. Failure sense:

Blase Ur, Xianzheng Guo, and Patrick Tague. Smartauth: Detecting sensor failure using electrical appliances in

User-centered authorization for the internet of things. the home. In 11th International Conference on Mobile Ad

In 26th USENIX Security Symposium (USENIX Security), Hoc and Sensor Systems (MobiHoc), pages 73?81, 2014

pages 361?378, 2017. [61] Dang Tu Nguyen, Chengyu Song, Zhiyun Qian, [72]

Rob van der Meulen and Janessa Rivera. Gartner says Srikanth V Krishnamurthy, Edward JM

Colbert, and a typical family home could contain more than

500 Patrick McDaniel. Iotsan: fortifying the safety of iotsys- smart devices by 2022.

Technical report, 2014. <http://www.gartner.com/newsroom/id/2839717>. In Proceedings of the 14th International Conference

//www.gartner.com/newsroom/id/2839717. on emerging Networking Experiments and Technologies [73]

Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl (CoNEXT), pages 191?203, 2018. Gunter.

Fear and logging in the internet of things. In [62] Sukhvinder Notra, Muhammad Siddiqi, Hassan

Habibi Network and Distributed System Security

Symposium Gharakheili, Vijay Sivaraman, and Roksana Boreli. An

(NDSS), 2018. experimental study of security and privacy risks with [74]

Rixin Xu, Qiang Zeng, Liehuang Zhu, Haotian Chi, Xi- emerging household appliances.

In IEEE conference on aojiang Du, and Mohsen Guizani.

Privacy leakage in communications and network security (CNS), 2014. smart homes and its

mitigation: Ifttt as a case study. IEEE Access, 7:63457-63471, 2019. [63] F. Pedregosa, G.

Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, [75]

Moosa Yahyazadeh, Proyash Podder, Endadul Hoque, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cour-
and Omar Chowdhury.

Expat: Expectation-based policy - napeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-

learn: Machine learning in Python.

Journal of Machine platforms.

In Proceedings of the 24th ACM Symposium Learning Research, 12:2825-2830, 2011.

on Access Control Models and Technologies (SACMAT), pages 61-72, 2019. [64]

Friedrich Pukelsheim. The three sigma rule. The American Statistician, 48(2):88-91, 1994. [76]

JuanYe,GraemeStevenson,andSimonDobson. Fault detection forbinary sensors in smarthome

environ- [65] EyalRonen,AdiShamir,Achi-OrWeingarten,andColin ments.

InPervasiveComputingandCommunications O?Flynn.

Iotgoesnuclear:Creatingazigbeechainreac- (PerCom),pages20?28,2015. tion.

In2017IEEESymposiumonSecurityandPrivacy [77]

JuanYe,GraemeStevenson,andSimonDobson. De- (S&P),pages195?212,2017. tecting

abnormal events on binary sensors in smart [66] Lee Russell. Wireless security monitoring

versus a homeenvironments. InPervasiveandMobileComput- cellularjammer. 2014.

ing,pages32?49,2016. USENIX Association 30th USENIX Security Symposium 4239[78]

QiangZeng,JianhaiSu,ChenglongFu,GolamKayas, A.2 TrainingandTestingResults Lannan

Luo,Xiaojiang Du,Chiu C Tan,and Jie

Wu. OnTestbed2,weextract32e2ecorrelationfromsmartapps Amultiversionprogramminginspiredapproachtod

pass 98 correlations from 2064 hypothetical correla- tecting audio adversarial examples. In

49th Annual tions. In total, we get 109 correlations after refining.

The IEEE/IFIP International Conference on Dependable Sys- difference of correlations regarding contact sensors, a

C1 on [79] Wei Zhang, Yan Meng, Yugeng Liu, Xiaokuan Zhang, the front door always gets

closed right after the accelera- Yinqian Zhang, and Haojin Zhu. HomeNit: Monitor-

tion is detected, while C2 and C3 are usually left open for incoming smart home apps from encrypted traffic.

In ACM a long time. The inaccurate correlation (cid:3) Epresence (PS2)

? away SIGSAC Conference on Computer & Communications Se-

Eswitch (L1) (cid:4) is accepted by the hypothesis testing. If not re- curity (CCS), pages 1074?1088, 2018.

off fined by the smart app rule R2.8, it causes 4 false alarms [80] Wei Zhou, Yan Jia, Yao

Yao, Lipeng Zhu, Le Guan, for HAWatcher (Mining Only) on case 2.3 and 2.6

when Yuhang Mao, Peng Liu, and Yuqing Zhang. Discovering only the resident taking PS2

leaves home. As detailed in and understanding the security hazards in the inter- our technical

report [44], HAWatcher achieves an aver- actions between IoT devices, mobile apps, and clouds

age detection precision of 94.85% and recall of 96.86%. In on smart home platforms. In 28th

USENIX Security terms of the false alarm test, HAWatcher raises 13

false Symposium(USENIXSecurity),pages1133?1150,2019.

alarmsamong6721eventscollectedwithinoneweek?test- ingperiod,whichcausesafalsealarmrate(FAR)of0.19%

ExperimentalResultsofTestbeds2to4 and1.86 false alarms perday. Among the 13 false

alarms, four (4) are raised by the correlations (cid:3)Eacceleration(C1) ? Table9:

Smartappsdeployedon Tesbeds2?4. R2.1,for

Emotion(MS1)(cid:4)and(cid:3)Eacceleration(C2)?Emotioa nct (i Mve

S2)(cid:4)because example,meansthefirstsmartappruleonTestbed2. active active

active ofstrongvibrationsintheneighborhoodthattriggerevents Index Smartapprules

oftheaccelerationsensorC1andC2. Three(3)areraised R2.1

IfMS2(active),thenP1(on)andL1(on)

by(cid:3)Eillumiance(L4)(cid:2)Smotion(MS3)(cid:4)becausetherearethree R2.2

IfMS2(inactive)for30minutes, low inactive thenP1(off),L1(off),L2(off),L3(off)

timesthataresidentremainsactiveinthestudyroomafter R2.3 IfMS3(active),thenL4(on)

thelightisturnedoff.Four(4)arecausedby(cid:3)Econtact(C3)(cid:2) R2.4

IfMS3(inactive)for10minutes,thenL4(off) closed R2.5

IfW(wet)orMS3(humidity?55),thenV(on)

Smotion(MS3)(cid:4)because residents close the door from outside. R2.6

IfV(on)for15minutes,thenV(off) active R2.7 IfPS1(present)orPS2(present),

Incontrast,theOCSVM-baseddetectorhasanaveragepre- thenturnonL1,L2,L5,P1

cisionof11.11%andrecallof35.41%with968falsealarms R2.8

IfPS1(away)andPS2(away), thenturnoffL1,L2,L3,L4,L5,V,P1

raised.TheARM-baseddetectorhasanaverageprecisionof R2.9 IfB(pressed),toggleL5

3.76%andarecall9.96%,andraises370falsealarms. R2.10

IfB(held),thenturnoffallLandP R2.11 IfB(doublepressed),turnonL1andL5andP1

OnTestbed3,HAWatcheraccepts50correlationsfrom527 hypotheses,and15e2ecorrelationsfromsmartapps.After

IfMS1(active)andMode(home),thenL1(on) R3.2 IfMS1(inactive)for60minutes,thenL1(off)

fining,thereare55correlationsleft.HAWatcherachievesan R3.3

IfB(pressed),toggleL1 averagedetectionprecisionof92.74%andarecallof93.36%. R3.4

IfB(held),thenL1(off)andMode(night) R3.5 IfB(doublepressed),thenL1(on)Mode(home)

Amongthetestingperiod,ten(10>falsealarmsareraised R3.6

IfPS(away),thenL1(off),P1(off),andMode(away)

byHAWatcheramong2411events,whichleadsto1.42false R3.7

IfPS(present),thenL1(on),P1(on),andMode(home) alarmsperdayonaverageandaFARof0.42%.Incontrast,the R

IfPS(away),thenP1(off)andP2(off) OCSVM-baseddetectorhasanaverageprecisionof31.01% R4.2

IfPS(present)thenP1(on),P2(on) R4.3 IfB(pressed),toggleP1

andarecallof42.33%,andraises379falsealarms.TheARM- R4.4 IfB(held),toggleP2 based

detector has an average precision of 9.89% and

an average recall of 14.10%, and raises 152 false alarms. A.1 Deployment

On Testbed 4, only 26 correlations are acquired because of the low density of IoT devices and smart apps. HA Watcher

9. On Testbed 3, the mode is used as a condition

to 90.17%. Five (5) false alarms are raised on this testbed among control the behavior of the light, while Testbeds 2 and 4

30th USENIX Security Symposium USENIX Association