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 ChenglongFu QiangZeng XiaojiangDu TempleUniversity

UniversityofSouthCarolina TempleUniversity chenglong.fu@temple.edu zeng1@cse.sc.edu

xjdu@temple.edu Abstract AsIoTdevicesareintegratedviaautomationandcoupled with the

physical environment, anomalies in an

appified smarthome,whetherduetoattacksordevicemalfunctions, mayleadtosevereconsequences.Priorworksth

Theminedcorrelationsarerefinedusing vicesmakeitpossibleforcyber-spaceattackstobeextended correlations

extracted from the installed smart apps.

The tothephysicalworld.AsshowninFigure1(a),thecommand refinedcorrelationsareusedbyaShadowExecution

?close the valve? is maliciously intercepted,which

may tosimulatethesmarthome?snormalbehaviors.Duringrun- causeroomflooding.Second,veryoftenadevicema

[15]couldresultinfiresbecauseofa testbedsandtestitagainsttotally62differentanomalycases. brokenrelay(anelec

Introduction

actionsofanother,whichfurtherexaggeratestheimpactof anomalies.AsshowninFigure1(c),asmartlockthatauto-

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

maticallyunlocksupontheresident?spresenceisunlocked homesgainboomingpopularity.AspredictedbyGartner,

duetoafakeeventofthepresencesensor. therewillbemorethan500IoTdevicesdeployedinatypical

Toaddresstheseconcerns,manyanomalydetectionsys- householdby2022[72].IoTdevicesbecomeincreasinglyin

tems[30,35,54,56,60,68,76]utilizedataminingtechniquesto tegrated,thankstoIoTplatformssuchasSmartThings

profilethesystem?snormalbehaviorsandreporteventsthat Homekit[47],andOpenHAB[55].Theseplatformsprov

deviatefromprofilesasanomalies.However,theseworks interoperabilityamonghomeIoTdevicesbydifferentven-

usuallytakeeventlogsasinputswithoutfullyconsidering dors,andallow them to workaccording to user-specified

eachevent?ssemantics,whichactuallymaybeacquiredfrom automationprograms(alsocalledsmartapps).

smartapps,devicetypes,anddevicefunctionalities.Thelim- USENIX Association 30th USENIX

Security Symposium

4223itationsarethreefold.First,thelogicofsomesmartappsis toocomplextobeminedaccurately,causingfalsenega

thus,theycanhardlybeexplainedandoften confuseusers.Third,thelearningresultscannotbeupdated quicklywhen

andcanberefinedeasilytoresolveconflictswithsmart appsandupdatedconvenientlywhenappschange. Intuitively

Weproposethenotionofshadowexecutionforsmart cations,canhelpimprovetheaccuracyofanomalydetection. ho

however,itisunknownhowto representthediversesemanticinformationintheformof ?

WeimplementaprototypeHAWatcherandevaluateit eventlogs.2)Systembehaviorpatternsderivedfromsmart

onfourreal-worldtestbeds.HAWatcherreachesahigh apps andthose minedfrom events logs

mayconflict. Itis

precisionof97.83%andarecallof94.12%,significantly challengingtoidentifyandresolvetheseconflicts.3)When outperformingpriorapproaches. smartappschange,therearenoeffectivemethodstoupdate thesystemprofilingacc

Therestofthepaperisorganizedasfollows.InSection2, To fill the gap, we present Home

Automation Watcher

wedescribebackgroundaboutappifiedsmarthomes.InSec- (HAWatcher),anovelanomalydetectionsystemforapp

tion3,wesurveyIoTdeviceanomaliesandpresentthethreat homeautomationsystems.Weproposeasemantics-assis

model.InSection4,wedescribethreecorrelationchannels miningmethodthatexploitsdiversesemanticinformation

andtherepresentationofcorrelations.Wepresentthedesign toconstructhypotheticalcorrelations(whereacorrelatio

detailsinSection5.TheevaluationispresentedinSection6. scribeshowadevicestateoreventcorrelateswithanother)

We discuss relatedworkin Section 7,andlimitations and anduseeventlogs asevidence to

verifythem. Second,as

futureworkinSection8.ThepaperisconcludedinSection9. thecorrelationsareexplainableaccordingtothesemantic

2 Background:AppifiedSmartHomes they can be easily refined to resolve conflicts with

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

IoTdevicesinsmarthomeshavebecomeincreasinglyinte- dated conveniently according to smart

app changes. The

gratedviaIoTplatformsforrichautomation.IoTintegration correlationsarethenusedbyourshadowexecutionmodu

platforms,suchasSmartThings,AmazonAlexa,andOpen- tosimulatenormalbehaviorsinthevirtualworld.Thesim

HAB,supporttrigger-actionautomationprograms.Onthese latedstatesarecomparedtothoseintherealworld

through

platforms,despitethehugenumberofIoTdevices,theyare bothcontextualcheckingandconsequentialchecking,and

abstractedintoasmallnumberofabstractdevices.

Forex- inconsistenciesduringcomparisonarereportedasanomalies.

ample,asmartlight,regardlessofitsbrand,shape,size,and Wemakethefollowingcontributions.

wirelesstechnology,isabstractedintothesameabstractde- vice,light.Eachabstractdevicehasitsassociatedeventsan

Weproposeanovelanomalydetectionsolutionforappi-

commands.Devicevendorscanhavetheirproductssupport fiedsmarthomes.Itmeetstheemergingneedofdetectintegrationbyrealizingtheeventsandcommands. inganomaliescausedbyIoTmalfunctionsorattacks.

WechooseSmartThings[21]asanexampleIoTintegra- tionplatformtopresentourdesign,asSmartThingsisoneof ?

Weproposeasemantics-assistedminingmethod,which

theleadingplatformsandsupportssophisticatedautomation infusesvarioussemanticinformation(smartapps,con-

logic.Otherintegrationplatforms,suchasAmazonAlexa, figuration,devicetypes,installationlocations)intothe

havesimilarstructures.AsillustratedinFigure2,atypical miningprocess.AnNLP-basedapproachisdeveloped

SmartThingsdeploymenthasacloud-centricarchitectureof todescribedevicerelationsforgeneratinghypothetical

fourlayers.OnthetopistheSmartThingscloud,wheresmart correlations. The mined correlations

are explainable, appsrunandinteractwithabstractedcapabilities.Thecloud 4224 30th USENIX

Security Symposium USENIX

Associationcommunicateswith IoTdevicesthroughthenetworkcon- states. Forexample,the loss

ofa presence-off eventcould nectionlayerthatusesvariouscommunicationtechniques

leavethedoorunlockedaftertheresidentleaveshome. such as WiFi,Zigbee,and ZWave. An IoT devices can

be CommandFailures.Theycorrespondtocommandsissued partitionedintothecyberpartandthephysicalpart.

The bytheIoTplatformsthatfailtobeexecutedbythetarget cyberpartmanagesinterfacesforhumansandbridgesthe

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

malfunc- thelatterfulfillsitsfunctionsinthephysicalworld.Taking tionsthatcausecommandstofailtoexecute,such

irresponsive[11].(2)Aphysical-partmalfunctionisequiv- Next,we describe some terms used in

SmartThings. A

alenttoamalfunctioninatraditional(i.e.,non-smart)device. devicehasoneormultiplecapabilities,eachcategorized

Forexample,abrokenelectricalrelayinsideasmartplug anactuator

orsensor.Eachcapabilitydefinesoneormore

canpreventtheplugfromcuttingoffthepowersupply[18], attributes.Forexample,asmartplugdevicehasanattribute

althoughfromtheperspectiveoftheIoTplatform,theplug ?switch?and,optionally,anattribute?power.?Eachattribu

hasbeenturnedoff. state(i.e.,value)isstoredonthecloudandupdateddueto events sent from the

IoT device. For example,the Smart- 3.2

AttacksonIoTDevices Thingsmultipurposesensorhasacapabilitycontactsensor,

WesurveytherecentworkonattacksagainstIoTdevices, whose attribute ?contact? changes from

?open? to ?closed?

andfindHAWatcherhasthepotentialtodetectthefollowing whenSmartThingsreceivesaneventof?contactclosed?

fivedifferenttypesofattacks. thesensor.Inaddition,thestateofanactuator?sattributeis Fake Events.

They are events maliciously injected by

at- updatedduetoafeedbackevent,whichissentbythedevice tackers.Fakeevents[80]maycausesevereconsequenc

Motivation,GoalsandThreatModel

fakepresence-oneventcanunlockthedoor. FakeCommands.Anattackermayinjectfakecommands IoTdevicesare

Interceptions. Events can be intercepted and

dis- andthenpresentourgoalsandthreatmodel. cardedbyattackers.E.g.,thehomesecuritysystemcanbe 3.1

IoTDeviceMalfunctions

mutedbyinterceptingthewindowanddoorsensors?wireless connectionstostopthemfromsendingsensorevents[66

Events. Faulty events referto incorrectvalues re- IoT device and, at least, launch the following

attacks.

(1) portedbyIoTdevices.Theycanbecausedbysensordefects StealthyCommands.Theattackercancontrolthedevi

Commands. They are widely discussed in

Smart- thedevice,itdoesnotexecutethecommandbutsendsback Things?userforum,dubbed?poltergeists?[6,12,1

GoalsandThreatModel Usersfrequentlyreportedtheirlightswereturnedonduring We aim to

detect both IoT device malfunctions described midnightmysteriously[13]. in Section 3.1 and

attacks in Section 3.2. We clarify

that EventLosses(orLargeDelays).Theyrefertoeventsthat HAWatchercanonlydetectattacksthatviolatecorrelati

a large delayon status update

[8],whichwas evadeourdetection,whichisdiscussedinSection8. confirmedbySmartThings[20].Eventlossesmay

1Iffeedbackeventsarenotmuted,itismuchlikeaFakeCommand. 

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.Whenauserreturnshome,thereshouldbe therearenomaliciousorconflictingrulesintheinstalled

consecutiveevents,suchas?presenceon?showingtheuser?s smartapps;howtodetectmaliciouslogic[71]andconfli

proximityand?contact-sensoropen?fordooropening. rules[28,34]aretwoseparateresearchproblems,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 bechangedtothevalueaisdenotedasE?(A)

,whileastate a densedeploymentinthenearfuture,weexploitscenarios

whichindicatesthatthedeviceB?sattribute?hasthevalue whereanIoTdevicehasoneormoreotherdevicesnearby

bisdenotedasS?(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 caseofr

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)

shouldbefollowedbytheeventEswitch(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 formofco-presentortemporallyrelatedevents[35,39,45,68]. is true. For example, (cid:3)E

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

nwitch(heater)(cid:4) Thesecorrelationscanbeattributedtotheexecutionofsmart

Epower(plug) meansthat,whentheevent

arises,thestate high apps[29],physicalinteractions[39]orusers?activities[45].

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

on correlationsandcategorizethemintothreechannelsbelow. Fortherepresentationofacorrelationinvolvingcondi

CorrelationChannels tions, its anterior event is combined with the

conditions usingthe???symbol.Forexample,(cid:3)EMotion?SPresence? active

present SmartAppChannel.Smartappsnotonlydirectlycause Eswitch(Light)(cid:4) means the

event EMotion, if the condition on

active correlationsbetweentriggersandactionsasprogrammed,

SPresenceistrue,shouldbefollowedbyEswitch(Light) . present on butalsoimplysomeextracorrelationsthatshouldbeconsid- WeshowinSection5thatthetwotypesofcorrelations,

implies a possible correlation

worthverification, thatcorrelateviadifferentchannels. thatis,?ifthelightisturnedon,thenthemotionshouldbein th

5

HAWatcherDesignandImplementation exclusivelyturnedonbythesmartapp. Wefirstintroducetheworkflowofa

Channel. Two devices can correlate via a

cer- tion5.1),andthendescribethemajormodulesinHAWatcher, tainphysicalproperty.First,anactuatordevice?sa

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

Correlation

Refining sensordevicesobservingthatproperty.Forexample,asmart (Section5.4),and4)AnomalyDetection(Sect

2Forsimplicityofdescription,withoutcausingconfusionwesometimes caleventandgeneratetemporallycorrelated

omitthedeviceIDsandusethesimplifiednotationsE?andS? . a b Figure4:ArchitectureofHAWatcher.

Figure5:DetectinganomaliesdepictedinFigure1. 5.1

WorkflowofAnomalyDetection TheAnomalyDetectionmodulerunsparallelwiththeappi- fiedhomeautomation,

Byapplyingsemanticanalysisto theapp,HAWatcherextractsane2ecorrelation(cid:3)Ewater

? detected Evalve

(cid:4).Sinceattackersintentionallyinterceptthecommand closed ?closethevalve?towardsthevalve,thereisnofee

the correlation. Furthermore,if Figure6:CodesnippetoftheappLightUpTheNight. closed it is a

Command Failure caused by the valve?s

cyber-part malfunction,HAWatchercandetectitthesameway.

(1).ItappliessymbolicexecutiontotheIntermediateRepre- In case (b),the hypothetical e2s

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

sentationofappsandcapturestheconfigurationinformation, Sswitch(cid:4)isfirstproposedbasedonthephysicalch

ticsofeachappisrepresentedasoneormorerules,eachin turning-off commandis sentto the plug

andexecutedby theformofatupletrigger(T)-condition(C)-action(A),which its cyber part (hence, its Switch=off), however, due to its meansthat?ifT occurs,whenC

istrue,executeA.? brokenrelay,theplugstillsuppliespowerandthusthepower

Step(2),whichconvertsrulestocorrelations,isstraight- meterreportseventsofhighpowerusage,whichviolatesthe

forward. Assuming T is reflectedbythe

eventE1,andE2 aforementionedcorrelationandtriggersanalarm.

isthefeedbackeventduetoexecutingA,theruleaboveis Incase(c),astheresidentdoesnotactuallyreturnhome,

convertedtoacorrelation(cid:3)E1?C?E2(cid:4). thereisnoeventE oc po en

ntactthatfollowsthefakeeventE pp rr ee ss ee nn tce .

TakingaSmartThingsofficialappLightUpTheNight [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)andisthusreportedasananomaly.

moduleconvertsitintotwoe2ecorrelations:(cid:3)E <Il 3lu 0minance? E oL

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

SemanticAnalysis tion(?Illuminance<30?or?Illuminance>50?)andthetrigger TheSemanticAnalysismoduleexe

eventin eachrule referto the same attribute ofthe

same semanticsfromsmartappsandtheirconfiguration,suchas

device;wethusmergethetriggerandtheconditiontoderive thetemperaturethresholdforturningonACandwhichIoT

aconciserepresentationofthetriggerevents. devicesareboundtowhichapp,and(2)convertthesemantics Moreover

tion(cid:3)E?(A)?E?(B)(cid:4)extractedfromthesmartapp,wefur- Semanticanalysis has been

usedto detectmalicious or a

b therproposeahypotheticale2scorrelation(cid:3)E?(B)(cid:2)S?(A)(cid:4), riskysmartapps as in

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

S?(A) scribedinourpriorwork[33,34]toextractsemanticsinStep whichmeansthattheevent

onlyariseswhen is b a USENIX Association 30th USENIX Security Symposium

4227true.Suchhypotheticale2scorrelationsarenot necessarily Table 1: Part of the adjacency

table. A cell marked

with true,andhavetobeverifiedusingeventlogs(Section5.3). (cid:2)meansthecorrespondingattributeinthecolum

CorrelationMining

relatewiththeoneintherowhead.Thefulltableof73*73 isinourtechnicalreport[44] Whilethereexistmanypatternm

CarbonDioxide Contact Illuminance Motion Power Presence Humidity Sound Button

Switch bothgoodusabilityandhighaccuracyinthecontextofappi- fiedhomeautomation.Supervisedminingmetho

more accurate but require well annotated datasets

or users?interventions.Unsupervisedmethods[31,35,60,68] canbeappliedtounannotateddata,butarelessaccurat

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-basedmining method. Semanticinformation 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) cludesdevices?typesandinstallationlocations,whichcan Power (cid:2) (cid:2)

(cid:2) beobtainedfromhomeautomationplatforms.Basedonthis 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,HAWatcherproposeshypotheticalcorrelations Sound (cid:2) (cid:2) (cid:2)

(cid:2) (cid:2) (inadditiontothosee2scorrelationsfromsmartapps)cor- Button (cid:2) (cid:2)

(cid:2) respondingtophysicalchannelsanduseractivitychannels. Switch (cid:2) (cid:2) (cid:2)

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

(cid:2) Eachhypotheticalcorrelationisthenverifiedindependently. Forphysicalchannelcorrelations,weconsiders

PrepossessingEventLogs

power,andairquality.TodeterminewhethertwoIoTdevice attributesmayrelateviaaphysicalproperty,wedevelopa

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

and a

physical designapreprocessingschemeforredundancyremovaland property,weuseGoogle?spre-trainedword2v

inthelistandthephysicalproperty,andusethehighestscore itsreadingsfromtheentiretrainingdatasetandcalculateit

astherelatednessscorebetweenthephysicalpropertyand mean?andstandarddeviation?.Readingsthatfalloutside t range [??3?,?+3?] are excluded as extreme values

tenattributeswiththehighestscores,whichareconsidered (i.e.,thethree-sigmarule[64]).3

Then,weapplytheJenks

mutuallycorrelatedviathatphysicalproperty. naturalbreaksclassificationalgorithm[49]4totheremaining Thiswa

device?s given attribute,we traverse the events

and inTable1.AsSmartThingsstipulates73attributes[19],the removethosethatdonotchangethestate(e.g.,consecu

tableis73*73.Acellwith(cid:2)meansthattheattributesinits EIlluminance).Now,eachtwotemporallyadjacenteve

rowheadandcolumnheadcorrelate. thesameattributeofadevicehaveoppositevalues. Whilemostofthecellsareaut

HypotheticalCorrelationGeneration

exceptionistheswitchattribute:asallactuatordeviceshave theswitchattribute,wemarkitascorrelatedwithallother 

andmotionasthetwospecialattributesthatdirectly useractivitychannelswithothersemanticinformation,such refle

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

all asdeviceattributesandrelationsbetweenattributes.Wefirst theattributes,intheadjacencytablewemarkpresenc attribute pairs; then,we fill each pair with

de- Foraspecificsmarthome,allattributesoftheinstalled vicesthathavematchingattributestogeneratehypothetical

may correlate. Given a pair of correlated

attributes 3Eventexclusionisfortrainingonly;theanomalydetectionmodule ? and ? in the

adjacency table,the device A with the at- doesnoteliminateevents.

tribute?,andBwith?,wegeneratefourhypotheticale2e resu4 lJ te sn fk os rn oa nt eu -r da il mb er

nea sik os na dlg ao tari [t 3h 8m ]andK-meansalgorithmgivethesame 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),andfoure2sones((cid:3)E a?(A)?S b?(B)(cid:4), 5.4

CorrelationRefining (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 Theacceptedhypotheticalcorrelationsshouldnotbeused aanda(cid:6) (bandb(cid:6)

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

overlooked if they remain unchanged during

training. erateanothereighthypotheticalcorrelationswiththeevents For instance, assume there is

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

sunset. Moreover,weproposetocombinesemanticsfromsmart If the residents always come

back home after sunset,the appswithsemanticsfromtheadjacencytable.Theintuition

(cid:3)Econtact

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

open

on beacceptedbyhypothesistestingandcausefalsealarmsof smartappisexecuted,itusuallyimposescertainchange

Second,whenappschange,acceptedhypothetical aconditionextractedfromasmartapp,wecreateavirtual correlati

present

correlationsextractedfromsmartapps,andlaunchthere- EMotion(M) arisesandPSispresent.Next,thevirtualdevic

fining process whenever smart app changes or there

are active isused,justlikethecorrespondingrealdevice,togenerate hypothetical correlations

accepted by hypothesis testing. hypotheticalcorrelationsaccordingtotheadjacencytable.

Wefirstdefinethecover relationbetweentwocorrelations: ane2ecorrelationC s=(cid:3)E a?(A)?E

b?(B)(cid:4)extractedfroma Our current prototype only considers devices

installed inthesameroomforgeneratinghypotheticalcorrelations. smartappcovers a correlation

C =(cid:3)E?(C) ?E?(D)(cid:4) that h c d Whilethiscanberelaxedbyconsideringanytwodevices

passes hypothesis testing if they meet two conditions:

1) inthehome,ourcurrentimplementationmakesatrade-off

theyhavethesameposteriorevent(i.e.,E?(B)=E?(D) );and betweenthecomprehensivenessofhypotheticalcorrelat

E?(A) E?(C) Eb ?(A) ?d E?(C) 2) (logically) implies (i.e., ).

If andthemeaningfulnessoftheminedcorrelations. a c a c C covers C ,the latter is removed. In the example men- s h tionedabove,asmartappderivede2ecorrelation(cid:3)E oc po en

ntact? 5.3.3 HypothesisTesting Slocation ?Eswitch(PorchLight)(cid:4) covers the

minedcorrelation Itisworthemphasizingthathypotheticalcorrelationsarenot sunset

on (cid:3)Econtact ?Eswitch(PorchLight)(cid:4) because theyhave the

same necessarilytrue.Thatiswhyweneedhypothesistesting,the open on posterioreventand(E oc

po en ntact?S sl uo nc sa et tion)?E oc po en

ntact;thus,the processofverifyinghypotheticalcorrelationsusingevent logs.Givenahypotheticalcorrelation,wetr

lattercorrelationisremoved. tofindalleventsthatmatchitsanterior,andtakeeachofthem 5.5

AnomalyDetection asatestingcase.Then,wecheckwhetherthehypothetical correlation?sposterioreventorstateis

constitutesatestingcasefor active

shadowexecutionengine,whichsubscribestotheeventsof thehypotheticalcorrelation(cid:3)E aM

cto it vi eon?E os

nwitch(Light)(cid:4).This theinstalledIoTdevices.Itkeepstrackofalldevices?states caseiscountedasasuccessifE andsimulatesasmarthome?slegitimatebehaviorsbasedon on shortdurationd

afterEMotion.Inourimplementation,d =

obtainedcorrelations. active 60s,whichislongenoughtowaitforthefeedbackeventto

Foreachincomingevent,theshadowexecutionengine arrivebutnottoolongastoacceptaneventnotrelatedto

performstheContextualandConsequentialcheckingsucces- EMotion.NotetheschedulinggranularityofSmartThi

occursinavalidcontextspecifiedine2scorrelations.After Checkingthesetestingcasescanbeconsideredasase-

that,theconsequentialcheckingsearchesforitsconsequen- quenceofindependentBernoullitrails.Weusetheone-ta

tialeventsaspredictedbye2ecorrelations. test[42]toevaluateeachhypotheticalcorrelation?scorrect-

Below,weusethesameexamplecorrelation(betweena ness.Foragivencorrelation,wesetthealternativehypothe-

motionsensorandalight)asinSection4.2.Whenanevent EMotion(A) sisH?as?thecorrelationsucceedswithaproba

isreceived,theshadowexecutionenginefirstcon- active than P0?. Correspondingly,the null

hypothesis H0 is ?the ductsthecontextualchecking.Ittraversesalle2scorrelations correlation

succeeds with a probability no higher than P0?.

andlocatesthosewiththeeventEMotion(A) attheiranterior Wechoosethe95%fiducialprobabilityasincommonpra

active places.Amongthelocatede2scorrelations,ifanyofthem tices [27],which means that the

correlation can only be have states in their posterior places that are

inconsistent acceptedifthenullhypothesis?sp-valueissmallerthan5%. USENIX Association 30th

USENIX Security Symposium 4229Table2:Numbersofrooms,devicesandappsineachtestbed.

Table3:IoTdevicesusedinthefourtestbeds,theirabbrevia- tionlabels,attributesanddeploymentinformation. Testl

#Rooms #Devices #Smartapps Abbr. DeviceName Attributes Deployment 1 5 23 17 2 4 19

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

4 Sensor illuminance, humidity W SmartThings water

onbathroomfloor withthereal-worlddevices?states,analarmisraisedreport-

WaterleakSensor EMotion(A) C SmartThings contact, ondoors ingtheevent

asinvalid.Otherwise,theeventis ContactSensor acceleration active B SmartThings button

bedside acceptedandtheshadowexecutionenginechangesitssimu- Button latedmotionsensor?sstateto?active?ac

L SmartThings switch

asceilinglight,lamp eachacceptedevent(motionAturns?active?intheexample), LightBulb PS

SmartThings presence inwallet the shadow execution engine performs the consequential

Arrivalsensor EMotion(A) P SmarThings switch,power

tocontrolfan, checking.Itsearchesalle2ecorrelationsthathave active SmartPlug

computer,andlamp attheiranteriorplacesandcacheseventsattheirposterior A Netatmo

carbonDioxide, onkitchen AirStation sound,humidity

countertop placesinawaitinglist.Ifanyeventinthelistisnotreceived V ThreeReality switch

tocontrolfan within60seconds(consistentwithd inhypothesistesting),

SmartSwitch theshadowexecutionenginereportsananomalyofamissing Table4:AutomationrulesusedinTestbed

Smartapprules eventfromitsderivedvirtualdevice(definedinSection5.3.2) iftheinvolvedconditionistrue,andthe

R1 IfM1(active)whenMode(home),thenP3(on) R2

IfM2(active)whenMode(home),thenP4(on) deviceishandledinthesamewayasthatfromtherealdevice

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 fortesting. 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.WecompareHAWatche

R17

IfPS1orPS2(present),thenturnonL1,L2,andP1andMode(home) otheranomalydetectors.Here,wemainlypresent

testbed,weletteresident(s)proposedesiredautomation, presentedinAppendixA.2. whichis

fulfilledby us withoff-the-shelfIoT devices

and smartappsfromtheSmartThingsofficialrepository.Wethen 6.1 ExperimentalSetup

givethemsufficienttimetogetfamiliarwiththeinstalled homeautomationbeforestartingdatacollection. Whilether

Deployment. The device deploymentis

depicted orhomeactivitylearningresearches,suchas[36,37],noneof inFigure7.Wedeploy10differenttypesofIoT

Table3,includingtheirabbreviation

labels.Note thesetestbedscontainmainlysensordevicesbutveryfew thattheThreeRealitySmartSwitch(denotedas

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

be Next,wedescribehowwesetupourtestbeds. usedtocontrolelectricalapplianceswithpowerplugs;for Testbeds

and Participants. We deploySmartThings

sys- example,inTestbed1,P1andP2areconnectedtoaTVand temsinfourhomesandTable2liststheirbasicinformat

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

Symposium USENIX

AssociationFigure7:Floorplansoffourtestbedsanddevicedeploymentlayouts(thedeviceabbreviationlabelsareill

Allparticipantsarefullyawareof

thebedroomdoor(withC3)doesnothavethispattern. alltheinstalleddevicesandapps.Wedonotuseanysensi-

Observation2:Thee2scorrelationC23meansthatMS3?s tivedevicessuchascamerasandmicrophones.Thesound i

asthehighillumi- andpersonalidentifiableinformation(PII)isremovedright nancevaluecanbecausedbymultiplel

isnotfollowedbyapower-highevent,asthe donottargetanysafety-sensitivedevices,suchasheaters.

on TVneedstobefurtherturnedonmanuallybytheresidents. Wenotifyparticipantsofincomingtestingonedayahea

Observation4:Physical-anduseractivity-channelcorrela- anomalycases.Wealsoaskparticipantstokeeptheirnorm

tionscannotbeobtainedwithoutmining,sincetheyarenot livinghabitsanddonotpaniciftheynoticeanyanomalies.

includedinanysmartapps.Ontheotherhand,somecorre- Thepurposeistoavoidtheirbehavioralbiasduringtesting.

lationscanbeeasilyextractedfromsmartappsbutdifficult Detailsoftheinjectedanomaliesarepresentedtoparticipa tomine.Forexample,correlationsthatinvolvedelaysare afterthetesting.

difficulttobeminedaccurately,butcanbepreciselyderived fromrules,suchasR4,R6,R8,andR10. 6.2

Training TrainingBaselineApproaches.WeselecttheAssociation TrainingHAWatcher.FromTestbed1,wegener

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

Vec- correlationsfromtheautomationrules.Inaddition,wegen- tor Machine (OCSVM) [67]

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

approaches. We choose OCSVM because it is

wiedly e2scorrelationsfromthesmartappchannel,544fromthe used foranomaly detection and

trained with one class of physicalchannel,and1,808fromtheuseractivitychannel.

inputdata,whichissuitableforourtrainingdatacontaining Then,thehypotheticalcorrelationsarecheckedusing22,6

no orfewanomalies [53]. ARM is selectedbecause itis a events collected from the three weeks?

training phase. In well-establishedmethodforminingcorrelations/rules,and total,146

correlations are accepted by hypothesis testing, HAWatcherisalsobasedoncorrelationmining. and130remainafterrefining.

Onotherthreetestbeds,the

WeperformARM[24]onthesametrainingdatasetfor portionofsmartappchannelcorrelationsare32/109,15/55,

comparison.SinceARMalgorithmsrequiretransaction-form and8/26,respectively. Table 5

listsa portion ofthe corre-

inputs,wesegmentthetrainingdatasetatplaceswherethe lationsafterrefining.Somecorrelationsrevealinteresting

timeintervalbetweentwoconsecutiveeventsislongerthan factsthatareconfirmedbytheresidents.

60s(thesameasthethresholddusedforhypothesistesting). Byusingthelibrarypymining[22],wemine221associatio

ruleswiththeconfidencethresholdof0.95.Unlikeourcor- active

relationminingmethodthatcoversvariousattributesand Econtact(C1)(cid:4),whichmeanstheeventEacceleration

active devices,rulesproducedbytheassociationruleminingare Econtact(C1) befollowedby .

Thisisbecausethefrontdoor

dominatedbymotionsensorsMS3andMS4.Allthe221rules closed (withC1)istypicallyclosedrightafterbeingope haveeitherMS3orMS4?smotionattributesintheirconse- USENIX Association 30th USENIX

Security Symposium 4231Table5:AportionofrefinedcorrelationsacquiredfromTestbed1. 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)?Eilluminance(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 T

Recall #offalsealarms #ofcorrelations

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

inthesmalldatasetswillcausesometruecorrelationstobe 6 75.35% 85.78% 147 141 rejected.Ontheotherhand,duetothesmallamountofdata, 9 94.57% 94.12% 15 135 12 97.25%

94.12% 8 132 manyfalsecorrelationsarenotrejectedyet.(3)Startingfrom 15 97.83% 94.12% 4

130 thedatasetof15days,theperformance(includingthenum- 18 97.83% 94.12% 4

130 beroffalsealarms)doesnotchangeanymore,whichmeans 21 97.83% 94.12% 4

130 thatamountofdataissufficientforthetestbed.(4)Thosetrue correlationswhichhavebeenrejectedinthesmallda

arerecoveredinthelargerdatasets.Thisshowstherobust- eventset.Thereare80rulesinvolvinglightsL4andL5,32

nessofthedesignofHAWatcher.Evenifveryfewanomalies withilluminancesensorsinMS3andMS4,and14withth

ariseduringthetrainingphase,truecorrelationscansurvive CO2sensorinA.Otherattributesarenotseeninanyrules,

givensufficienttrainingdata.(5)Weexaminethedifferent aseventsinvolvingthemareovershadowedbythoseinvol

setsofcorrelationsminedbasedondifferentdurationand ingthefouraforementionedattributes.Incontrast,withour

find that some false correlations remain there until

more dataisavailable.Forexample,(cid:3)Ehumidity(MS3)(cid:2)Scontact(C3)(cid:4) miningmethod,eachattri

closed correlationsandhasanaverageof10.5correlations.

remainsuntilbehaviorsthatfailthecorrelationappearon FortheOCSVM-baseddetector,ittakesasnapshotofall

Days11and12. devices?statesasaframeeachtimeaneweventarisesand concatenatesfourconsecutiveframesasone

6.3 AnomalyGeneration tor

[48].WeusetheopensourceOCSVMimplemetationin sklearn[63]andthedefaultkernel(RadialBasisFunction).

ToevaluateHAWatcher,wesimulate24casesofanomalies onTestbed1listedinTable7(totally62casesonthefour In

We follow two criteria to select anomaly

cases: ofthedurationofthetrainingphaseontheperformanceof (1)theattacksarediscussedintheliteratureaboutIoTS

either modify the testing event logs (collected in

the asatrainingdataset,andthenusethefirstsix(6)daysby fourthweek)orinterferewiththehomeautomation,andthe

Faulty/FakeEvents.Wesimulatethembyinsertingevents correlationsthanthesubsequentones,theoverallquality

ofdevices,suchasmotionsensors[17],presencesensor[14], of correlations is not high. The

reason is that we use the andcontactsensors[3],astheyarereportedlyunreliable. 4232 30th

AssociationTable7:HAWatcher?sdetectionperformanceonTesbed1.?#inst.?indicatesthenumberofinstancesfor

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 togglefromtheghostsmartapp 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 numberof

alarms reporting

that beenfrequentlyreportedbyusersforturningon/offunex- anomalycase(i.e.,ratiooftrueanomaliestoalarms),rec

smartapp,whichisnot is the numberofcorrectly detectedinstances

ofthatcase knownbyHAWatcher,andusetheapprandomlyissuecom- dividedbythenumberofinjectedinstancesof

rate is the numberoffalse positives

dividedbythe StealthyCommandsWithcompromisedsmartlights[65]

numberofIoTevents. andplugs[58],attackerscancontrolthemtomakestealthy buthazardousactions.Wesimulatet

Precision=

TruePositive TruePositive+FalsePositive thesamemethodasghost/fakecommandsbutremovethe feedbackeven

Recall= TruePositive (1) TruePositive+FalseNegative Command Failures (cyber)/Command

Interceptions FalseAlarmRate=

FalsePositive WesimulateCommandFailures(cyber-partmalfunctions)

AllEvents andCommandInterceptionsonsmartplugs[11]andsmart DetectorsforComparison.Wecomparetheper

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 CommandFailures(physicalpartmalfunctions)andDenialof takeasnapshotofalldevices?statesasaframe

Association 30th USENIX Security Symposium

4233thebenefitbroughtbythecombinationofthetwo,webuild

missedinstancesshouldnotimposehazards,astheevents twovariantsofHAWatcher:HAWatcher(AppsOnly),whi

areconsistentwiththefactthattheresidentsareactivedur- extractscorrelationsfromsmartappsonly,andHAWatcher

ingthetime.Similarly,the26missedinstancesofCase10 (MiningOnly),whichminescorrelationswithoutusingapps

areilluminancereadingswhichhavesimilarvalueswithreal readingsatthetime.ForCase9,twoinstancesaremissed

Results of HAWatcher. As shown in Table

7, becausetworesidentsarebackhometogetherwhenoneof HAWatcherhasanaveragedetectionprecisionof97.83

Below we describe some examples to illustrate howHAWatcherdetectsanomalies.

Comparison.(1)AsshowninFigure8,HAWatcherachieves DetectingCase7.Residentsentering/leavingthebedroo

thebestperformanceacrossallthe24cases.(2)HAWatcher openthedoor,whichisinstalledwithanaccelerationsen-

(AppsOnly)merelyobtainse2ecorrelationsfromsmartapps, sor C3, and cause the motion-active

event of MS3. How- andcanonlydetectanomalies,suchasCommandFailures ever,as

motion-active events of MS3 are intercepted/lost,

(cyber)/CommandInterceptions.Itgets16.67%forboththe theuseractivitye2ecorrelationC17=(cid:3)Eaccelerati

hasthesecondbest performance.Onaverage,itsprecision active

is88.42%andrecall88.62%,showingtheeffectivenessand DetectingCase11.Ghost/FakeCommandsthattrytoturn

ofourmining 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

lackofknowledgeofsmartapps,itmissesmanyinstances is derived from the on >950

ofCases2,11,12,and20.(4)TheARM-baseddetectorhas smartappruleR14andacceptedbythehypothesistesting. a anomaly instances for 17 of the 24 cases,as its

rules ofapps,butitwouldbedifficult,ifnotimpossible,forpure coververyfewattributes(Section6.2).(5)OCSVMpe

turn on the plug P2 to start the connected

fan,which notfallinsidethesameinputvector. Epower(P2) causes the event . However,Since the

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

isinterceptedbyattackers,theswitchofP2 on

HAWatcherusingthetestingeventlogs(collectedduringthe Sswitch(P2) isstillatthestate

.Thus,thephysicalchannele2s

fourthweek).Weconsideranyalarmsthatarenotduetoour off correlationC6=(cid:3)Epower(P2)(cid:2)Sswitch(P

anomalyinjectionandcannotbecategorizedasanyofthe high

on anomalytypeslistedinSection3asfalsealarms.HAWatcher DetectingCase20.CommandFailures(cyber)/Com

totally 13 anomalies other than those injected

by Interceptionsaredetectedbecauseofviolationofthesmart appchannele2ecorrelationC38=(cid:3)E am co tit vio en(M2)?S hm oo md ee? u tis o. nA sCm 1o 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 ofcorrelations C20 andC21,because

ofthe on Incontrast,HAWatcher(MiningOnly)cannotlearnthiscor-

largedelaysofsomeeventsfromtheaccelerationsensors. relationandthusmissesallinstancesofthiscase.

SuchanomaliesarecategorizedastruepositivesduetoEvent Detecting Case 21. L1 accepts the

turning-on command LossesorLargeDelays(Section3.1).Theyshouldbereported and sends the

feedback event,but due to a physical-part

tousers,asthelargedelaymayconfuseusersandevencause failureorDoE,thelightisnoton.Whilemostoftheinstance

undesiredautomation(e.g.,anunlock-doorcommandarrives of Case 21 can be detected as

violation of the correlation

lateaftertheuserhaslockedthedoor). C24=(cid:3)Eilluminance(MS1)(cid:2)Sswitch(L1)(cid:4)(sincetheillumin off keepslowbutthelight-switchstateison),3instancesare

twoareduetoviolationofC4andC5,becausethereisone missed,becausetheroomhasbeenbrightenedupbynatural

timethattheresidentsstayedoutsidethedoorforawhile light(hence,illuminancehasalreadybeenhigh)whenthe

(longerthan60seconds)beforeopeningthefrontdoor;C11 anomalyarises.

andC18eachcauseonefalsealarm,andthereasonisthat For Cases 1,3,6,9,and 10,some instances

are missed,

theresidentsleftthefrontdooropenforquiteawhileand whichshouldbeattributedtoimperfectionofanomalysim-

thenclosedit.Whileitisarguablewhetheranomaliesdue ulation(ratherthantheinabilityofHAWatcher).Forexam-

touserbehavioraldeviationsshouldbecategorizedasfalse ple,seveninstancesofCase1aremissed,becausethefake

alarms,weconsiderthemfalsealarms,astheyarenotdue motion-activeeventsofMS1happentobeinjectedduring

toattacksordevicemalfunctions. Emotion(MS1) the time when there are real events of ; such

Intotal,HAWatcherreportsfour(4)falsealarmsfrom9,756 active 

AssociationFigure8:RecallandprecisionofHAWatcherandfourotherdetectorsforcomparisonpurposes. eventsco

malware,ratherthanIoTmalfunctions.Forexample,Home- perdayandafalsealarmrateof0.04%.Incomparison,AR

Guard[33,34]presentsthefirstsystematiccategorization andOCSVMcause722and1,116falsealarms,respectively

ofthreatsduetointerferencebetweendifferentautomation thatis,103and159perdayandfalsealarmrates7.40%and

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

automationconflicts,chainedexecution,andlooptriggering; itisalsothefirstthatusesSMTsolverstosystematically

PerformanceuponSmartAppChanges tectsuchthreats.Itconductssymbolicexecutiontoextract automationrulesf

an appified home,it is common that users change

the smartapps,suchasinstallingnewappsandchangingthe

PFirewall[32]isauniqueworkthatnoticesexcessiveIoT configuration.However,traditionalminingbasedanomaly

devicedatacontinuouslyflowstoIoTautomationplatforms. detection needs a long time to adapt

to the changes and,

Itenforcesdataminimization,withoutchangingIoTdevices duringtheadaptationtime,maytriggermanyfalsealarm orplatforms,toprotectuserprivacyfromplatforms. Handlingsuchchangesforanomalydetection in

appified IoTSan [61] statically analyzes smart apps to

predict homeshasbeenchallenging.Weconductsmartappchange whether the resulting

automation may violate any safety experimentstoevaluateHAWatcher?sperformanceandcom-

properties.

IoTGuard[29]instrumentssmartapps.Before pareitwithothersystems,OCSVMandARM.

anappissuesasensitivecommand,theactionhastopass As listed in Table 8, we create five cases

of smart app

thepoliciesdefinedbyusers.Bothrelyonpre-definedpoli- changes,whichcoverchangesoftrigger,condition,action

cies,while HAWatcherdoes not. Unlike

ourwork,which andthewholerule.Foreachcase,weuseonedaytocollect

detectsIoTdeviceanomalies,HoMonit[79]isfocusedon thedata,andthenapplyHAWatcher,OCSVM,andARMto

detectingmisbehavingsmartapps.Givenaphysicalevent, thecollecteddata.TheresultsshowthatHAWatcherdoes

Orpheus[31]checksthesystemcalltraceduetotheevent nottriggeranyalarms,whileOCSVMtriggersmanyalarms

against an automaton to detect attacks; it cannot detect forallthe five cases andARM forthe

changes of R8 and

anomaliessuchasfakeevents,eventinterceptions,etc. R10.Wemanuallyinspectthealarmsandconfirmthatthey

Manyanomalydetectiondetectorslearnnormalbehaviors areallfalsealarmscausedbyappchanges.

ofasmarthomefromitshistoricaldata[26,35,51,54,60,69, ARMdoesnottriggerfalsealarmsforthechangesof

R3, 75,76].Forexample,SMART[51]trainsmultipleuseractiv- R5,and R14 because it does not

include any association

ityclassifiersbasedondifferentsubsetsofsensorreadings, rulescoveringthedevices,suchasL1andL3,involvedinth

and further trains another classifier that takes the

vector updatedrules.FortheOCSVM-baseddetector,eachvector

ofactivity-classificationresultsasitsinputtodetectsensor containsfourconsecutivesnapshotsofdevicestates.Inthe

failures.DICE[35]detectsanomaliesduringstatetransitions Eswitch(L1) bycheckingthecontext.Peeves[26]makesuseofdatafrom caseofR3,forexample,themissing

causesunseen on anensembleofsensorstodetectspoofedevents. vectorsandthustriggersfalsealarms.ForHAWatc

RelatedWork

Notonlyisthedetectionmoreaccurate,buteachdetected anomalycanbeinterpretedasaviolationofacorrelation, Wi

whichitselfisexplainable.Priortoourwork,itisunclear 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].

complexbehaviorsinanappifiedhome(e.g.,Testbed1with Mostofthemarefocusedondetectingthreats,attacksand

17apps).HAWatcherprovidesaneffectivesolution. Table8:Thenumberoffalsealarmscausedbysmartappchanges. OriginalRule Type

Ruleafterchange HAWatcher OCSVM ARM R3 Actionchange

IfMS1(active),thenL2(on)andL1(on) 0 14 0 R5 Newrule

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 smartthings.com/en/latest/ref-docs/smart

[2] Lights follows me, 2015.

https://github.com/ thecorrelationsmayconstructattacksthatdonotviolateany

SmartThingsCommunity/SmartThingsPublic/tree/ correlationsinordertoevadedetection.Thebottomlineof

master/smartapps/smartthings/light-follows-me.src. runningHAWatcheristhatitimposesextraconstraintsonat-

Doorknockergoing crazy,2016.

https://community. tackers.InTestbe1,eachattributeisinvolvedinatleastfour smartthings.com/t/door-knocker-g

[4] Tons of issues with smartthings, 2016.

https: anyofthecorrelations.Forexample,giventhecorrelation

//www.reddit.com/r/SmartThings/comments/ (cid:3)Elock(frontdoor)(cid:2)Spresence(cid:4)(i.e.,thefrontdoo

present canonlyarisewhenthepresencesensorison),ifanattacker

smartthings/. hascompromisedthedoorlock,analarmwillbetriggeredif [5] When st glitches become major safety fire haz- theattackerunlocksthedoorwhennobodyishome. ard, 2016.

https://community.smartthings.com/t/ SparselyDeployedIoTDevices.SomeIoTdevicesmight when-st-glitches

sparsely deployed, and physical-channel correlations 43109. among them might be very few.

A promising solution is toexplorethecorrelationsintheentirehome,ratherthan [6] Are the

poltergeists back?, 2017. inseparaterooms,whichcanhopefullyderivemorecorrela-

https://community.smartthings.com/t/october- tionsamongdevices.Moreover,itisatrendthatIoTdevices

2017-are-the-poltergeists-back-devices-randomly- aredeployedwithincreasingdensity.

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

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

https://www.smartthings.com. 2017.

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

Pymining-acollectionofdataminingalgorithmsin python,2020.

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

https://community.smartthings.com/t/ [23] Troubleshooting: Smartthings

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

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

2017.

us/articles/200955940-Troubleshooting-SmartThings- https://community.smartthings.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.smartthings.com/t/smartthings-

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: Fabian Monrose. Sok:

Security evaluation of home- //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.smartthings.com/t/undesired- Peeves:Physicaleventverificationinsmarthomes

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

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

KateCalder. Statisticalinference.

NewYork:Holt,1953. whats-wrong-with-smartthings-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

ATC), //ficara.altervista.org/?p=3744&doing_wp_cron= pages147?158,2018. 1591921359.510802030563354

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

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://smartthings. flow control for home automation systems.

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

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

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

threats in smart homes: https://support.smartthings.com/hc/en-us/articles/

Categorization,detectionandhandling.

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,andJiaping Zhang,andPatrickTague. Doyoufeelwhatihear? Yu.

Cross-app interference threats in smart homes:

enablingautonomousiotdevicepairingusingdifferent Categorization,detection and handling. In

50th An- sensortypes.

In2018IEEESymposiumonSecurityand nualIEEE/IFIPInternationalConferenceonDependable

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-

pherMPoskitt,andJunSun. Anomalydetectionfora man, Karthik Gopalratnam, Sira Rao,

Andrey Litvin, watertreatmentsystemusingunsupervisedmachine andFarhanKhawaja.

Mavhome:Anagent-basedsmart learning. In2017IEEEInternationalConferenceonData home.

InProceedingsoftheFirstIEEEInternationalCon-

MiningWorkshops(ICDMW),pages1058?1065,2017. ferenceonPervasiveComputingandCommunications (Pe

[49] GeorgeFJenks. Thedatamodelconceptinstatistical mapping.

Internationalyearbookofcartography,7:186? [38] BordenDent.

Cartography?thematicmapdesign.1999. 190,1967. pages147?149. [50]

YunhanJackJia,QiAlfredChen,ShiqiWang,AmirRah- [39] Wenbo Ding and Hongxin Hu. On

the safety of

iot mati,EarlenceFernandes,ZMorleyMao,AtulPrakash, devicephysicalinteractioncontrol.

InProceedingsof andShanghaiJiaoTongUnviersity.

Contexiot:Towards the2018ACMSIGSACConferenceonComputer&Com- providingcontextualintegritytoapp

NancyElHadyandJulienProvost.

Asystematicsur- veyonsensorfailuredetectionandfault-tolerancein [51] Krasimira Kapitanova,

Enamul Hoque, John A ambientassistedliving. Sensors,18(7):1991,2018. Stankovic, Kamin

Whitehouse, and Sang H Son. Beingsmartaboutfailures:assessingrepairsinsmart [41]

EarlenceFernandes,JaeyeonJung,andAtulPrakash. homes.

InProceedingsofthe2012ACMConferenceon Securityanalysisofemergingsmarthomeapplications. Ubiquitous

StylianosPKavalarisandEmmanouilSerrelis. Security [42] RonaldAylmerFisher.

Statisticalmethodsforresearch issuesofcontemporarymultimediaimplementations: workers. In

Breakthroughs in statistics,pages 66?70. Thecaseofsonosandsonosnet.

InTheInternational Springer,1992.

ConferenceinInformationSecurityandDigitalForensics (ISDF),pages63?74,2014. [43] Milan

Fránik and Milo? ?ermák. Seri- ous flaws found in multiple smart home [53]

ShehrozSKhanandMichaelGMadden. One-classclas- hubs: Is your device among them?,

2020.

sification:taxonomyofstudyandreviewoftechniques. https://www.welivesecurity.com/2020/04/22/serious-

TheKnowledgeEngineeringReview,29(3):345?374,2014. flaws-smart-home-hubs-is-your-device-among- [54

PalanivelAKodeswaran,RaviKokku,SayandeepSen, them/. andMudhakarSrivatsa. Idea: A

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

failuremanagementinsmartiotenvironments. InPro- Hawatcher: Semantics-aware anomaly

detection ceedings of the 14th Annual International Conference for appified smart homes

(technical report), 2020.

onMobileSystems,Applications,andServices(MobiSys), https://github.com/infinitywings/HAWatcher.git.

pages43?56,2016. [45] JunHan,AlbertJinChung,ManalKumarSinha,Mad- [55] K Kreuzer.

Openhab-empowering the smart home, humithaHarishankar,ShijiaPan,HaeYoungNoh,Pei

2013. 4238 30th USENIX Security Symposium USENIX Association[56] Wenke Lee, Salvatore J Stolfo, and Kui W Mok. A [67]

BernhardSchölkopf,JohnCPlatt,JohnShawe-Taylor, data mining frameworkforbuilding

intrusion detec- Alex J Smola,and Robert C Williamson. Estimating tionmodels.

InProceedingsoftheIEEESymposiumon thesupportofahigh-dimensionaldistribution.

Neural SecurityandPrivacy(S&P),pages120?132,1999.

computation,13(7):1443?1471,2001. [57] XiaopengLi,QiangZeng,LannanLuo,andTongboLuo.

[68]

AmitKumarSikder,HidayetAksu,andASelcukUlu- T2Pair:SecureandUsablePairingforHeterogeneous

agac. 6thsense:Acontext-awaresensor-basedattack IoTDevices.

InProceedingsoftheACMConferenceon detector for smart devices. In 26th USENIX

Security Computer&CommunicationsSecurity(CCS),2020.

Symposium(USENIXSecurity),pages397?414,2017. [69] Amit KumarSikder,Leonardo

Babun,HidayetAksu, [58] HaoyuLiu,TomSpink,andPaulPatras.

Uncovering andASelcukUluagac.

Aegis:acontext-awaresecurity securityvulnerabilitiesinthebelkinwemohomeau- frameworkforsmarthomesyste

InProceedingsof tomationecosystem.

In2019IEEEInternationalCon- the35thAnnualComputerSecurityApplicationsConfer- ferenceonPervasiveCon

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

TomasMikolov,IlyaSutskever,KaiChen,GregSCor- RoksanaBoreli.

Smart-phonesattackingsmart-homes. rado, and Jeff Dean. Distributed representations

of InProceedingsofthe9thACMConferenceonSecurity& words and phrases and their

compositionality. In PrivacyinWirelessandMobileNetworks(WiSec),pages Advances in

neural information processing systems 195?200,2016. (NeurIPS),pages3111?3119,2013. [71]

YuanTian,NanZhang,Yueh-HsunLin,XiaoFengWang, [60] Sirajum Munir and John A

Stankovic. Failuresense:

BlaseUr,XianzhengGuo,andPatrickTague.Smartauth: Detectingsensorfailureusingelectricalappliancesin

User-centeredauthorizationfortheinternetofthings. thehome.In11thInternationalConferenceonMobileAd

In26thUSENIXSecuritySymposium(USENIXSecurity), HocandSensorSystems(MobiHoc),pages73?81,2014

pages361?378,2017. [61] Dang Tu Nguyen, Chengyu Song, Zhiyun Qian, [72]

RobvanderMeulenandJanessaRivera. Gartnersays Srikanth V Krishnamurthy,Edward JM

Colbert,and a typical family home could contain more than

500 PatrickMcDaniel.Iotsan:fortifyingthesafetyofiotsys- smartdevices by2022.

Technicalreport,2014. http: tems.InProceedingsofthe14thInternationalConference

//www.gartner.com/newsroom/id/2839717. onemergingNetworkingExperimentsandTechnologies [73]

Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl (CoNEXT),pages191?203,2018. Gunter.

Fearandloggingintheinternetofthings. In [62] Sukhvir Notra, Muhammad Siddiqi, Hassan

Habibi Network and Distributed System Security

Symposium Gharakheili,VijaySivaraman,andRoksanaBoreli. An

(NDSS),2018. experimentalstudyofsecurityandprivacyriskswith [74]

RixinXu,QiangZeng,LiehuangZhu,HaotianChi,Xi- emerginghouseholdappliances.

InIEEEconferenceon aojiangDu,andMohsenGuizani.

Privacyleakagein communicationsandnetworksecurity(CNS),2014. smarthomes andits

mitigation: Iftttas a case study. IEEEAccess,7:63457?63471,2019. [63] F. Pedregosa, G.

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

MoosaYahyazadeh,ProyashPodder,EndadulHoque, R.Weiss,V.Dubourg,J.Vanderplas,A.Passos,D.Cour-

andOmarChowdhury.

Expat:Expectation-basedpol- napeau,M.Brucher,M.Perrot,andE.Duchesnay.Scikit-

icyanalysisandenforcementforappifiedsmart-home learn:MachinelearninginPython.

JournalofMachine platforms.

InProceedingsofthe24thACMSymposium LearningResearch,12:2825?2830,2011.

onAccessControlModelsandTechnologies(SACMAT), pages61?72,2019. [64]

FriedrichPukelsheim. Thethreesigmarule. TheAmer- icanStatistician,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/IFIPInternationalConferenceonDependableSys- differenceofcorrelationsregardingcontactsensors,a

C1on [79] WeiZhang,YanMeng,YugengLiu,XiaokuanZhang, the front dooralways gets

closedright afterthe accelera- YinqianZhang,andHaojinZhu. Homonit: Monitor-

tionisdetected,whileC2 andC3 areusuallyleftopenfor ingsmarthomeappsfromencryptedtraffic.

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

? away SIGSACConferenceonComputer&CommunicationsSe-

Eswitch(L1)(cid:4)isacceptedbythehypothesistesting.Ifnotre- curity(CCS),pages1074?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 YuhangMao,PengLiu,andYuqingZhang. 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- actionsbetweeniotdevices,mobileapps,andclouds 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?stest- 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)Eilluminance(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)becauseresidentsclosethedoorfromoutside. 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%andarecallof9.96%,andraises370falsealarms. R2.10

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

OnTestbed3,HAWatcheraccepts50correlationsfrom527 hypotheses,and15e2ecorrelationsfromsmartapps.Afte

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 averagerecallof14.10%,andraises152falsealarms. A.1 Deployment

OnTestbed4,only26correlationsareacquiredbecauseof thelowdensityofIoTdevicesandsmartapps.HAWatcher

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

to 90.17%.Five(5)falsealarmsareraisedonthistestbedamong controlthebehavioroftheligh t,whileTestbeds2and4