IoTSan: Fortifying the Safety of IoT Systems

Dang Tu Nguyen*, Chengyu Song*, Zhiyun Qian*, Srikanth V. Krishnamurthy*,
Edward J. M. Colbert†, and Patrick McDaniel‡

*UC Riverside, †U.S. Army Research Laboratory, ‡The Pennsylvania State University

Abstract

Today’s IoT systems include event-driven smart applications (apps) that interact with sensors and actuators. A problem specific to IoT systems is that buggy apps, unforeseen bad app interactions, or device/communication failures, can cause unsafe and dangerous physical states. Detecting flaws that lead to such states, requires a holistic view of installed apps, component devices, their configurations, and more importantly, how they interact. In this paper, we design IoTSan, a novel practical system that uses model checking as a building block to reveal “interaction-level” flaws by identifying events that can lead the system to unsafe states. In building IoTSan, we design novel techniques tailored to IoT systems, to alleviate the state explosion associated with model checking. IoTSan also automatically translates IoT apps into a format amenable to model checking. Finally, to understand the root cause of a detected vulnerability, we design an attribution mechanism to identify problematic apps. We evaluate IoTSan on the Samsung SmartThings platform. From 76 manually configured systems, IoTSan detects 147 vulnerabilities. We also evaluate IoTSan with malicious SmartThings apps from a previous effort. IoTSan detects the potential safety violations and also effectively attributes these vulnerabilities to malicious apps.

CCS Concepts

- Security and privacy → Software security engineering;
- System and software → Model checking.

ACM Reference Format:

Dang Tu Nguyen*, Chengyu Song*, Zhiyun Qian*, Srikanth V. Krishnamurthy*,

1 Introduction

A variety of IoT (Internet-of-Things) systems are already widely available on the market. These systems are typically controlled by event-driven smart apps that take as input either sensed data, user inputs, or other external triggers (from the Internet) and command one or more actuators towards providing different forms of automation. Examples of sensors include smoke detectors, motion sensors, and contact sensors. Examples of actuators include smart locks, smart power outlets, and door controls. Popular control platforms on which third-party developers can build smart apps that interact wirelessly with these sensors and actuators include Samsung’s SmartThings [73], Apple’s HomeKit [4], and Amazon’s Alexa [3], among others.

While conceivably, IoT is here to stay, current research studies on security/safety of IoT systems are limited in two fronts. First, they focus on individual components of IoT systems: there are papers on the security of communication protocols [24, 31, 40, 57, 70], firmware of devices [1, 15, 21, 72, 81, 90], platforms [28, 51], and smart apps [27, 28, 51, 83]. Very few efforts have taken a holistic perspective of an IoT system. Second, most current research efforts only focus on securing the cyberspace, and do not address the safety and security of the physical space, which is one of the key obstacles for real-world IoT deployment [60].

Our thesis is that a holistic view of an IoT system is important i.e., the distributed sensors and actuators, and the apps that interact with them need to be considered jointly. While the compromise of an individual component may lead to the compromise of the whole system, certain complex security and safety issues are only revealed when the interactions between components (e.g., a plurality of poorly designed apps) and/or possible device/communication failures are considered. These latent problems are very real since apps are often developed by third-party vendors without coordination, and are likely to be installed by one or more users (e.g., family members) at different times. Moreover, both legitimate device failures [29, 33, 86, 88] (e.g., from battery depletion) and induced communication failures (e.g., via jamming [69]) can lead to missed interactions between autonomous components, which in turn can cause the entire system to transition into a bad state. These issues are especially dangerous, because bad or missed interactions can be deliberately induced by attackers via spoofing sensors [76, 79], luring users to install malicious apps [51], or jamming sensor reports.

Goals: In this paper, our goal is to build a holistic system which, given an IoT system and a set of default plus user-defined safety properties with regards to both the cyber and physical spaces, (a) finds if components of an IoT system or interactions between components can lead to bad states that violate these properties; and, (b) attributes the detected violations to either benign misconfigurations or potential malicious apps. With regards to (a) we account for cases wherein app interactions or failed device(s)/communications...
can cause a bad state. With regards to (b) we look for repeated instantiations of unsafe states since malicious apps are likely to consistently try to coerce the IoT system into exploitable bad states (e.g., those described in [51]).

To achieve our goal, we need to solve a set of technical challenges. Among these, the key challenge lies in the scope of the analysis: as the number of IoT devices and apps is already large and is only likely to grow in the future [35, 49], physical replication and testing of IoT systems is hard (due to scale). Thus, it is desirable to build a realistic model of the system, which captures the interactions between sensors, apps, and actuators.

Our solution: We achieve our goal by addressing the above and other practical challenges, in a novel framework IotSan (for IoT Sanitizer). In brief, IotSan uses model checking as a basic building block. Towards alleviating the state space explosion problem associated with model checking [18], we design two optimizations within IotSan to (i) only consider apps that interact with each other, and (ii) eliminate unnecessary interleaving that is unlikely to yield useful assessment of unsafe behaviors. We also design an attribution module which flags potentially malicious apps, and attributes other unsafe states to bad design or misconfiguration.

We develop a prototype of IotSan based on the Spin model checker [43] and apply it to the Samsung SmartThings platform. As one contribution, we design an automated model generator that translates apps written in Groovy (the programming language of SmartThings apps) into Promela, the modeling language of Spin. To evaluate IotSan, we postulate 45 common sense safety properties and consider 150 smart apps with 76 configurations. With this setup, IotSan discovered 147 violations of 20 safety properties due to app interactions (135 violations) and device/communication failures (12 violations). In an extreme case, 4 smart apps needed to interact to cause a violation, which is extremely difficult to spot manually. We evaluate our attribution module with 9 malicious apps from [51] that are relevant to our problem scope (e.g., causing bad physical states). IotSan attributes all 9 apps to be potentially malicious. A summary of our contributions is as follows:

- We map the problem of detecting potential safety issues of an IoT system into a model checking problem. We develop novel pre-processing methods to alleviate the state explosion problem in model checking.
- We design IotSan to detect safety violations in IoT systems and develop a prototype that applies to the Samsung SmartThings platform. We provide the source code of IotSan for download at https://github.com/dangtunguyen/IoTSan 1. We develop tools to automatically translate the app source code into Promela. We evaluate IotSan with 150 smart apps from the SmartThings‘ market place and discover 147 possible safety violations.
- We propose a method to attribute safety violations to either bad apps or misconfigurations. The method attributes 9 known malicious apps with 100% accuracy.

2 BACKGROUND AND SYNOPSIS

Today’s IoT systems [3, 4, 48, 56, 63, 73, 85] typically consist of three major components viz., (i) a hub and the IoT devices it controls, (ii) a platform (can be the hub, a cloud backend, or a combination) where smart apps execute, and (iii) a companion mobile app and/or a web-based app to configure and control the system. Without loss of generality, we design IotSan assuming this underlying architecture. Therefore, although the implementation of IotSan is tailored to the SmartThings platform given its recent popularity, [13, 14, 27, 28, 51, 83], conceptually IotSan is also applicable to other IoT platforms. We use the term “IoT system” to refer to those used in smart homes as in recent papers such as [13, 14, 27, 28, 51, 83] for ease of exposition; however, our approach can apply to other application scenarios (e.g., IoT based enterprise deployments or manufacturing systems [23, 45, 58, 64]).

2.1 Samsung SmartThings

Overview: Like the other systems mentioned above, SmartThings has an associated hub and a companion mobile app, that communicate with a cloud backend via the Internet, using the SSL protocol [6]. Developers can create smart apps using the Groovy programming language. The platform and apps interact with devices through device handlers; written in Groovy, these are virtual representations of physical devices that expose the devices’ capabilities. To publish a device handler, a developer needs to get a certificate from Samsung. Typically, smart apps and device handlers are executed in the SmartThings cloud backend inside sandboxes.

Programming model: A smart app subscribes to events generated by device handlers (e.g., motion detected) and/or controls some actuators using method calls (e.g., turn on a bulb). Smart apps can also send SMS and make network calls using the SmartThings’ APIs. A smart app can discover and connect to devices, in two ways. Typically, at installation time, the companion app shows a list of supported devices to a user; after configuration, the list of the user’s chosen devices are returned to the app. The second (lesser-known) way is that SmartThings provides APIs that allow apps to query all the devices connected to the hub. Besides subscribing to device events, smart apps can also register callbacks for events from external services (e.g., IFTTT [46]) and timers.

Communications: The hub communicates with IoT devices using a protocol such as ZWave or ZigBee. Experiments using the EZSync CC2531 Evaluation Module USB Dongle [47] of Texas Instruments, reveal that the ZigBee implementation in SmartThings supports four (single hop) MAC layer retransmissions. In addition, SmartThings has an application support sublayer that performs 15 end-to-end retransmissions (for a total of 60 retransmissions of a packet). These are in line with ZigBee specifications as also verified in [2, 8, 53, 59]. Thus, typically, it is rare that the system will transition to unsafe states because of benign packet losses.

2.2 Misconfiguration Problems

Besides malicious apps, misconfiguration is a common cause for safety violations. When installing a smart app, a user has to configure the app with sensor(s) and actuator(s). Poor configurations can transition the IoT system to unsafe physical states. There are many common causes for such misconfigurations, e.g., (i) the app’s description is unclear, (ii) there are too many configuration options, and (iii) normal users often do not have good domain knowledge to clearly understand the behaviors of smart devices and smart

1A more detailed technical report is also available at this site.
The problem of reasoning if and why the IoT system could transition into a bad physical state is challenging because the number of apps and devices is likely to grow in the future and thus, analyzing all possible interactions between them will be hard. Static analysis tools tend to sacrifice completeness for soundness, and thus result in lots of false positives. In contrast, typical dynamic analyses tools verify the properties of a program during execution, but can lead to false negatives.

Model checking is a technique that checks whether a system meets a given specification [50], by systematically exploring the program’s state. In an ideal case, the model checker exhaustively examines all possible system states to verify if there is any violation of specifications relating to safety and/or liveness properties. However, the complexity of modern system software makes this extremely challenging computationally. So in practice, when the goal is to find bugs, a model checker is usually used as a falsifier i.e., it explores a portion of the reachable state space and tries to find a computation that violates the specified property. This is sometimes also called bounded model checking [10, 20, 26, 52, 61].

We adopt model checking as a basic building block since: (i) it provides the flexibility towards verifying all the desired properties with linear temporal logic\(^2\), (ii) it provides concrete counter-examples [5, 80] which are very useful in analyzing why and how the bad states occur, (iii) its holistic nature of checking can capture interactions among multiple apps, and (iv) it is more efficient than exhaustive testing [9]. However, a successful model checker must address the state explosion problem, i.e., the state space could become unwieldy and requires exponential time to explore.

Given its popularity and flexibility in modeling both concurrent and synchronous systems [17, 25, 54], we use Spin [43] for checking if a given set of safety properties can be possibly violated. Since an IoT system may be composed of a large number of apps and smart devices, we use Spin’s verification mode with BITSTATE hashing—an approximate technique that stores the hash code of states in a bitfield instead of storing the whole states. Although the BITSTATE hashing technique does not provide a complete verification, empirical results and theoretical analysis have proved its effectiveness in terms of state coverage [12, 16, 41, 42, 44].

### 3 Scope and Threat Model

In this work, our goal is to detect safety issues (i.e., vulnerabilities) of IoT systems that are exploitable by attackers to transition the system into bad physical states or leak sensitive information. Safety requirements (i.e., definition of bad states and information leakage) can come from both the users and security experts. Examples of bad physical states are (i) the front door is unlocked when no one is at home, and (ii) a heater is turned off when the temperature is below a predefined threshold. With regards to information leakage we require that: (i) private information is sent out via only

---

\(^2\) Linear temporal logic (LTL) is a modal temporal logic with modalities referring to time. LTL is used to verify properties of reactive systems [5].
message interfaces (e.g., sendSmsMessage and sendPushMessage in SmartThings) but not via network interfaces (e.g., httpPost in SmartThings), and (ii) the recipients of methods for sending messages may be unrelated event handlers.

We consider all devices (hub, sensors, and actuators), the cloud, and the companion app as our trusted computing base (TCB), and do not consider software attacks against them. However, IoTSan does mitigate physical attacks that can inject event(s) into the system (e.g., by physically increasing the temperature or spoofing the sensors) or maliciously induced device or communication failures (e.g., by jamming [69]). IoTSan seeks to identify and prevent such events from leading the system into safety violations. However, targeted solutions to those attacks (e.g., preventing spoofing of sensors or jamming mitigation) are out-of-scope.

We also consider potential bad states that can arise due to natural device failures. Note that many users have reported the failures of their ZigBee and Z-Wave IoT devices (e.g., motion sensors, water leak sensors, presence sensors, and garage door openers) in the SmartThings Community [29, 33, 86, 88]. Failures could also result from device batteries running out. We seek to identify if such device failures can cause an IoT system to transition into a bad physical state.

Malicious apps can exploit weaknesses in the configuration and attack other apps by introducing problematic events. We only seek to attribute an app as possibly malicious and leave the confirmation to human experts or other systems.

4 SYSTEM OVERVIEW

Figure 2 illustrates a high level view of the chain of events in an IoT system. In brief, sensors sense the physical world and convert them into events in the cyber world; these events, in turn, are passed onto apps that subscribe to such events. Upon processing the cyber events these apps may output commands to actuators, passed onto apps that subscribe to such events. Upon processing them into events in the cyber world; these events, in turn, are sent to human experts or other systems.

Figure 3 depicts the architecture of our system IoTSan. It consists of five modules viz., App Dependency Analyzer, Translator, Configuration Extractor, Model Generator, and Output Analyzer. In designing IoTSan, we tackle two main challenges: (i) alleviating the state space explosion with model checking [18] for our context, and (ii) the translation of smart apps’ source code to Promela (to facilitate model checking). We address the first problem partially in the App Dependency Analyzer and partially in the Model Generator. The second problem is handled partially in the Translator and partially in the Model Generator.

App Dependency Analyzer (§ 5): This module constructs dependency graphs to capture interactions between event handlers of different apps and identifies handlers that must be jointly analyzed by the model checker. This precludes the unnecessary analysis of unrelated event handlers.

Translator (§ 6): We build a translator within IoTSan, that automatically converts Groovy programs into Promela. In doing so, we address the following challenges:

- Implicit Types. In Groovy programs, data types of variables and return types of functions are not explicitly declared. To solve this problem, we design an algorithm to infer data types of variables and return types of functions.
- Built-in Utilities. Groovy has many built-in utilities, e.g., find, findAll, each, collect, first, + on list types, and map. We manually analyzed the behavior of each utility and translated them into corresponding code in Promela.

Configuration Extractor (§ 7): IoT platforms often provide a companion mobile app and/or web-based app to manage/configure the installed smart apps and devices of an IoT system. This module automatically extracts the system’s configurations from the manager app.

Model Generator (§ 8): This module takes the Promela code of event handlers, the configuration of the IoT system, and safety properties (both pre-defined and user-defined) as inputs, and creates the Promela model of the system. We use sequential design to model the IoT system instead of concurrent design. This significantly reduces the problem size by eliminating unnecessary interleaving that is unlikely to yield useful assessment of unsafe behaviors. The generated model is checked by Spin for possible property violations.

Output Analyzer (§ 9): This module analyzes the verification logs and attributes safety violations to potentially malicious apps, bad designs or misconfiguration. Based on the result, it provides the user, a suggestion to either remove a bad app(s) or change an app(s)’s configuration.

Our work in perspective: IoTSan can be envisioned as a service that jointly considers the apps, devices and their configurations of an IoT system, and checks whether a set of a priori defined properties hold. In addition to detecting safety violations of the physical

---

Table 1: Comparison of IoTSan and related work.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IoTSan</th>
<th>MPT</th>
<th>DoLoreum</th>
<th>Soteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detects physical safety violations</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Detects information leakage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detects violations due to communication/device failures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detects violations due to misconfiguration problems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handles complex code beyond IFTTT rules</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Performs violation attribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts for app interactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The model checker should not have to check the interactions between event handlers that do not interact. To find event handlers that can interact and thus jointly influence actuator actions, this module constructs a dependency graph (DG).

Extracting input/output events: Each smart app registers one or more event handlers that get notified of events to which it has subscribed. An event handler takes one or more input events, and can induce zero or more output events. Input events are (i) explicitly declared in the subordinate commands or, (ii) identified via APIs that read states of smart devices, or (iii) indicated by interrupts at specific times defined by schedule method calls. Output events are invoked via APIs that change states of smart devices. We enumerate the input and output events of an app using static analysis (details are straightforward and are omitted to save space).

Dependency Graph Construction: Once the input and output events are identified, we construct a directed DG as follows. Each event handler is denoted by a vertex in the DG. An edge from vertex u to vertex v (u → v) is added if the output events of u overlap with the input events of v. u is then called the parent vertex of the child vertex v. The vertices in a strongly connected component are merged into a composite vertex (a union of input and output events). A leaf vertex does not have any child.

Example: To illustrate, consider the following example. Table 2 summarizes the event handlers and the associated input/output events with a set of sample smart apps. The description of an event is in the format attribute/event type (e.g., contact/open means “a contact sensor is open”); empty quotes (“…””) denote “any” event of that type. Given these apps, the model checker automatically verifies i when j is verified; thus, there is no need to re-verify i. In Table 3c and Figure 4b, we show the final related sets associated with the DG in Figure 4a after removing all redundant subsets. These related sets are jointly analyzed by the model checker.

Related sets: The initial related set of a leaf vertex v ∈ DG includes all of its ancestors and v itself. There is no need to find such related sets for vertices that are not leaves, since those sets are subsets of other leaves’ related sets. Table 3a shows the initial related sets in the DG from Figure 4a.

The initial related sets constructed as above are incomplete. This is because, two vertices u and v may have common output events but the types of these events could be different or what we call conflicting. For example, nodes 0 and 1 have conflicting output events viz., switch/off and switch/on. In such cases, the related sets to which u and v belong, must be merged to account for such conflicts. Table 3b shows the related sets of vertices with potential output conflicts in our example. Note here that to check for such output conflicts, we need to examine O(E^2) links in the worst case (given E output edges from the event handlers); our experiments show that such checks are very fast.

We point out that if a related set i is a subset of a bigger related set j, the model checker automatically verifies i when j is verified; thus, there is no need to re-verify i. In Table 3c and Figure 4b, we show the final related sets associated with the DG in Figure 4a after removing all redundant subsets. These related sets are jointly analyzed by the model checker.

6 TRANSLATOR

Given its popularity and ease of use [32, 34, 75, 82], we build IoTSan using the Bandera Tool Set [37, 38], which is a collection of program analysis, transformation, and visualization components designed to apply model-checking to verify Java source code. Bandera generates a program model and specification in the language of one of several existing model-checking tools (including Spin, dSpin, SMV, JPF). When a model-checker produces an error trail, Bandera renders the error trail at the source code level and allows the user to step through the code along the path of the trail while displaying values of variables and internal states of Java lock objects [37, 38].

Since Bandera does not handle Groovy code, in order to analyze smart apps for SmartThings, we need to convert their code into Java which is challenging for the following reasons. First, since SmartThings added several language features to Groovy to simplify smart app development, the standard Groovy compiler cannot directly process an app’s code and SmartThings’s compiler is not open sourced. Second, Groovy uses dynamic typing [36] (i.e., data types are checked at run-time) but Java is static typed (i.e., data types are explicitly declared and checked at compile-time). Thus, we need to perform type inference during the translation of Groovy into Java. Lastly, Groovy supports many built-in utilities such as list and map, not supported by Bandera (i.e., Bandera supports only Java’s array type).

The key component we develop is the G2J Translator (see Figure 5), which translates the smart app Groovy source into Java’s Abstract Syntax Trees (ASTs). In addition, the SmartThings Handler is designed to handle the new language syntaxes introduced by SmartThings, and the GParser parses the regular Groovy source code into Groovy ASTs. Basically, each smart app in Groovy is translated into a Java class, whose method comprises of a method’s header and a block of statements. The translation procedure of a block is straightforward: iterate through the statement list of the
Table 2: An example to showcase the construction of a dependency graph.

<table>
<thead>
<tr>
<th>App’s Name</th>
<th>Event Handler</th>
<th>Vertex’s ID</th>
<th>Input Events</th>
<th>Output Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brighten Dark Places</td>
<td>contactOpenHandler</td>
<td>0</td>
<td>contact/open, illumiance/&quot;...&quot;</td>
<td>switch/on, switch/off</td>
</tr>
<tr>
<td>Let There Be Dark!</td>
<td>contactHandler</td>
<td>1</td>
<td>contact/&quot;...&quot;</td>
<td>switch/on, switch/off</td>
</tr>
<tr>
<td>Auto Mode Change</td>
<td>presenceHandler</td>
<td>2</td>
<td>presence/&quot;...&quot;</td>
<td>location/mode</td>
</tr>
<tr>
<td>Unlock Door</td>
<td>appTouch</td>
<td>3</td>
<td>app/touch</td>
<td>lock/unlocked</td>
</tr>
<tr>
<td>Big Turn On</td>
<td>changedLocationMode</td>
<td>4</td>
<td>location/mode</td>
<td>lock/unlocked</td>
</tr>
</tbody>
</table>

Table 3: Related sets of the dependency graph in Figure 4a:
(a) Initial related sets, (b) Potential conflicting sets, and (c) Final related sets.

(a) | (b) | (c)
---|---|---
Set Vertices | Set Vertices | Set Vertices
1 | 0 | 1 | 0, 1 | 1 | 3
2 | 1 | 2 | 1, 5 | 2 | 2, 4
3 | 5 | 3 | 1, 2, 5 | 3 | 1
4 | 5 | 4 | 1, 5 | 4 | 1, 5
5 | 2, 4 | 5 | 1, 2, 6 | 5 | 1, 2, 6

Grey boxes are existing modules/packages. The SPIN Trans module in Bandera is modified.

Figure 5: lOtSan is built around Bandera.

input Groovy block, translate each Groovy statement into Java, add the result to a list of Java statements, and build a Java block from the result list. To implement these, we extended the Groovy compiler (org.codehaus.groovy) which is then integrated into the Bandera’s front-end.

Handling SmartThings’ language features: There are several new language syntaxes introduced in SmartThings. Our SmartThings Handler parses these new syntaxes and converts them into vanilla Groovy code using specifications based on the domain knowledge of SmartThings. For instance, (as can be seen in in Figure 1) each input function defines a global variable (or a class field) of the app. Therefore, we traverse the Groovy’s AST of the app and visit all input functions to extract all global variables of the app. In addition, apps can use some predefined objects or variables (e.g., location) and APIs (e.g., setLocationMode), which are not defined in vanilla Groovy. Therefore, we manually add definitions of these global objects.

Type inference: Although the Groovy Compiler org.codehaus.groovy already has a sub-package CompileStatic for performing static type inference, it only works when the argument type and the return type of a method are given. In other words, a variable declared inside a method can take different runtime types depending on the argument type. Thus, we still need to infer the argument and return type statically. To do so, we consult the calling context of each method invocation by recursively tracking the arguments and return values to their corresponding anchor points—declaration of variables with explicit types (Groovy supports static typing as well), assignment to constant values (e.g., we can infer that the type of variable a is numeric from def a = 0), assignment to return values of known APIs, and known objects and their properties. The inference procedure works roughly as follows. When traversing the AST of a method, we store the names and data types of variables at anchor points; the types of other variables are inferred by propagating the types from anchor points. This is done iteratively until we find no more new variables whose type can be inferred.

Handling Groovy’s built-in utilities: Another challenge arises when we translate Groovy into Java for use with Bandera. We find that Bandera understands only a very basic set of Java. For instance, it supports only the array type natively. In contrast, Groovy’s collection types (e.g., Collection, List, ArrayList, Set, Map, and Hashset) all need to be translated into Java’s array type. We support the popular collection types that are commonly used in smart apps. An example is shown in Figure 6 that translates one Groovy list into a corresponding Java implementation using array. Since the type of
switches and onSwitches is List of STSFunctions, we infer the return type of onSwitches() method as List of STSFunctions, which is translated into Java’s array type (i.e., STSFunction[]. The + operator on List type (line 2 in Figure 6a) is automatically translated into corresponding Java’s code (lines 2-17 in Figure 6b). Finally, since this method is a non-void method, we add an explicit return statement (line 18 in Figure 6b).

7 CONFIGURATION EXTRACTOR

IoT platforms typically provide a mobile companion app and/or a web-based app to manage and configure smart apps and devices. For Samsung SmartThings, we develop a crawler in Java, using the Jsoup package to automatically extract the system’s configuration from the management web app [78]. Given a SmartThings account (user’s name and password), the crawler logs in to the management web app and extracts (i) installed devices, (ii) installed smart apps, and (iii) configurations of apps. Moreover, whenever a user installs a new generic smart device (e.g., a smart power outlet), we have an interface to get the device association info (e.g., this new outlet is used to control an AC) from the user. The extracted configuration is then saved to a file and used later by the Model Generator. The process is straightforward and we omit the details in the interest of space.

8 MODEL GENERATOR

Modeling an IoT system: To correctly verify safety properties, we need to model two key components (not part of the app code): (i) the IoT platform and its interactions with smart apps and (ii) IoT devices and their interactions with smart apps. IoT platforms [3, 4, 46, 63, 73] typically provide apps with some methods to register callback functions (i.e., event handlers). Based on apps’ configurations provided by the Configuration Extractor, we model these special registration functions so as to invoke callbacks at appropriate times.

We model IoT devices (sensors and actuators) as per their specifications. Note that both sensors and actuators can generate events of interest to apps. For instance, a motion sensor can generate motion active/inactive events whereas a door lock (actuator) can generate status update events (locked/unlocked). Each device is modeled as having an event queue and a set of notifiers to inform the smart apps that have subscribed to specific types of events. Currently, we support 30 different IoT devices. Note here that we model events generated by the environment (e.g., sunrise and sunset) as sensor generated inputs and location mode changes (e.g., Home, Away, and Night) as actuators; thus inputs such as users leaving home (sensed input) can trigger the mode to change from Home to Away (actuation).

We model system time as a monotonically increasing variable. We extract the triggering times and callback functions from the scheduling method calls. The callback functions are then triggered at appropriate times based on the value of the modeled system time.

Algorithm 1 shows the pseudo code of the main process that models behaviors of an IoT system. The model checker enumerates all possible permutations of the input physical events up to a maximum number of events per user’s configuration to exhaustively verify the system. At each iteration, a sensor and a corresponding physical event in the permutation space are selected (line 2). Then, the selected sensor updates its state and event queue, and notifies its subscribers of the state change event (line 3). When an event is pending, it is dispatched to the subscribed apps and the corresponding event handlers of apps are invoked to handle the event (lines 4-6). Each event handler may send some commands to some actuators, which may generate some new events and trigger event handlers of the subscribers.

To model natural or induced (e.g., using jamming [69]) device/communication failures, when generating a sensor event we enumerate two scenarios: (i) the sensor is available/online and (ii) the sensor is unavailable/offline. Similarly, whenever receiving a command from a smart app, an actuator may be either online or offline. If a device is offline, it will not change its state and hence not broadcast a state change event to its subscribers. If a device is online,

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of properties</th>
<th>Sample property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermostat, AC, and Heater</td>
<td>5</td>
<td>Temperature should be within a predefined range when people are at home</td>
</tr>
<tr>
<td>Location mode</td>
<td>3</td>
<td>Location mode should be changed to Away when no one is at home</td>
</tr>
<tr>
<td>Security and alarming</td>
<td>14</td>
<td>An alarm should strobe/siren when detecting smoke</td>
</tr>
<tr>
<td>Water and sprinkler</td>
<td>3</td>
<td>Soil moisture should be within a predefined range</td>
</tr>
<tr>
<td>Others</td>
<td>5</td>
<td>Some devices should not be turned on when no one is at home</td>
</tr>
</tbody>
</table>

CoNEXT ’18, December 4–7, 2018, Heraklion, Greece
the communication (i.e., sending a state change event or receiving a command) between the device and the hub/cloud may either succeed or fail (we enumerate both cases).

**Concurrency Model:** Since an app’s event handler is only triggered by the subscribed event(s) and event handlers of different apps do not share any global variable [3, 4, 46, 63, 73], the execution of an app’s event handler can be considered as atomic. This means that the concurrency level of a model only depends on the interleaving of apps’ event handlers. To model a concurrent IoT system therefore, we only need to verify the behaviors of the system with interleavings of all of the external events (e.g., smoke detected) sensed by sensors and internal events (e.g., unlocked) caused by apps’ behaviors. Even though the events are concurrent, the interleaving is in fact reflected by the order of the (incoming) events processed by event handlers, i.e., we can obtain the strict concurrency by considering all order permutations of external and internal events. However, this approach takes a very long verification time as the number of events grow, and causes the state space to explode. Instead, we can obtain a weaker concurrency by considering the permutations of only external events in a sequential design shown in Algorithm 1. This implicitly assumes that the internal events associated with an external event are handled atomically in order. It is unclear if enforcing strict concurrency would lead to the discovery of more unsafe states. We experiment with the two design options with several small systems and find that the sequential approach offering weak consistency, discovered all violations that the strict concurrent model found. Based on this, we use the sequential approach given that it significantly mitigates the time complexity of execution.

**The IoT system model in Promela:** With the concurrent approach, each device and smart app is modeled by a process (i.e., proctype). There is also a process for generating the sensed and environmental events. The processes communicate with each other using message passing (i.e., chan). We use a single process for the whole system with our sequential design, using inline methods to model the behavior of devices and smart apps. The devices, smart apps, and event generators, communicate via shared global variables.

**Safety Properties:** We seek to verify 45 properties of the following types:

- **Free of conflicting commands** [68]: When a single external event happens, an actuator should not receive two conflicting commands (e.g., both on and off) – (1 property).
- **Free of repeated commands:** When a single event happens, an actuator should not receive multiple repeated commands of the same type or with the same payload – (1 property). The latter could indicate a potential DoS or replay attack.
- **Safe physical states:** Table 4 shows some sample safe physical states that the user desires the system to satisfy. These kinds of properties can be verified using linear temporal logic (LTL) [5] – (38 properties). We envision that a more complete list will likely be provided by safety regulations associated with the IoT industry in the future.
- **Free of other known suspicious app behaviors—security-sensitive command and information leakage:** Examples of security-sensitive commands are unsubscribe (disabling an app’s functionality) and creating fake events (e.g., an app may generate a “smoke detected” event when there is no smoke in the physical environment); we raise violations when such commands are executed. Information leakage can occur with sending SMS and using network interfaces. When sending SMS is triggered, for instance, we check whether the recipient matches with the configured phone number to prevent leakage – (4 properties).
- **Robustness to device/communication failure:** An app should quickly check that a command sent to an actuator was acted upon to be robust to device and communication failures. Upon detecting a failure, the app should notify users via SMS/Push messages. This property can be verified using LTL as well – (1 property).

Note that we provide users with an interface to select the list of safety properties they want to verify. Based on the device association information (recall § 7) provided by the Configuration Extractor, the LTL format of the selected properties are automatically generated.

**Example:** Consider the smart home of a single owner Alice (say), which comprises of a smart lock that controls the main door viz., Door Lock, and a presence sensor viz., Alice’s Presence (which checks if Alice is at home). Assume that Alice installs two smart apps: Auto Mode Change, which manages the location mode based on the events from Alice’s Presence and, Unlock Door, which unlocks the Door Lock based on explicit user input or a “location mode” change event. When this system is analyzed by the model checker, a violation is detected as described below.

Figure 7 shows the (filtered) violation log (a counter-example) output by SPIN. The format of each line in the violation log is as follows: file name (SmartThings0.prom), line number, state number, and the executed code. In particular, the counter example has the following steps. (1) The event not present is generated by Alice’s presence if Alice leaves home (line 1) and its subscribers are notified of this state change (line 2). (2) The app Auto Mode Change reads and processes this state change event (lines 3-5) and notifies the location manager to change the location mode to Away (line 6). (3) The location manager changes its mode and notifies its subscribers of this change (lines 7-8). (4) The app Unlock Door reads and processes this mode change event (lines 9-10) and sends an unlock command to the device Door Lock (line 11), which unlocks the door (lines 12-13). Thus, the system enters an unsafe physical state (i.e., the main door is unlocked when no one is at home) (lines 14-15).

Upon closer inspection, the description of Unlock Door suggests that it unlocks the door only upon user input. However, in practice, it also unlocks the door whenever the location mode changes (i.e., there is an inconsistency between the app’s description and its implementation).

### 9 OUTPUT ANALYZER

The Output Analyzer attributes a violation to either a misconfiguration or a malicious app using a heuristic-based algorithm. The algorithm consists of two phases. In the first phase, when a user installs a new smart app, the output analyzer enumerates all possible configurations for this app. It verifies if the user-defined properties hold with each configuration independently. If the proportion of
violations (violation ratio) is greater than a predefined threshold (e.g., 90%), the new app is attributed as a malicious app.

If this is not the case, in the second phase, the new app is verified in conjunction with other apps that were previously installed by the user. Again, all configurations are considered. If the violation ratio is greater than a predefined threshold, the new app is attributed as a bad app and a report is provided to the user. Otherwise, the violation is attributed to misconfiguration and suggestions of safe configurations with regards to the user defined properties are provided. If there is no violation, a successful verification is reported.

10 EVALUATIONS

Our experiments (model checking) are performed on a MacBook Pro with macOS Sierra, 2.9 GHz Intel Core i5, 16 GB 1867 MHz DDR3, and 256 GB SSD. We check if there are violations of the properties discussed in §8. We also look at other performance metrics such as the running times, and the scale ratio (which quantifies the reduction in the number of event handlers to be jointly verified) to evaluate IotSAN.

10.1 Test Cases and Configurations

We perform four different sets of experiments described below. The first three examine the fidelity with which bad apps and configurations are identified. The last set evaluates the performance of different design choices we make.

Market apps with expert configurations: We check the safety properties with 150 apps (assuming they are benign) from the SmartThings’ market place [19, 77, 78]. We (the authors) came up with independent configurations for the apps (based on common sense with regards to how the apps may be used). To illustrate, consider the app Virtual Thermostat, the required input to which is shown in Figure 1. Assume that the following devices are deployed: (1) one temperature sensor (myTempMeas), (2) one outlet to control the heater (myHeaterOutlet), (3) one outlet to control the air conditioner (myACOutlet), (4) one outlet to control the light in the living room (livRoomBulbOutlet), (5) one outlet to control the light in the bedroom (bedRoomBulbOutlet), (6) one outlet to control the light in the bathroom (bathRoomBulbOutlet), (7) one motion sensor in the living room (livRoomMotion), and (8) one motion sensor.

Figure 7: Example violation log (filtered).
10.2 Identifying Unsafe Configurations

Market apps with expert configurations: Table 5 summarizes the results from our first set of experiments in the absence of device and communication failures. The apps in parenthesis jointly cause a violation. We find 38 violations of 11 properties, some of which can be very dangerous from a user’s perspective. For example, there is violation where “The main door is unlocked when people are sleeping at night”, which involves 4 apps. The interactions between the apps that lead to this violation is shown in Figure 8a: when lights are turned off at night a mode change is initiated by the Good Night app, which in turn causes the unsafe action of unlocking the main door by the UnLock door app.

Device/communication failures cause violations of 9 additional properties with some dangerous cases. One such case is showcased in Figure 8b. When people leave home, the Make it so app should automatically lock the entrance door; however, due to the failure of the motion sensor, the Make it so app is not triggered and thus, the door is left unlocked. Moreover, this failure also causes NO notification to be sent to law enforcement upon physical intrusion. An alarming discovery is that none of the analyzed apps check if the commands sent to the actuators were actually carried out. That is violation where “The main door is unlocked when no one is at home and, when smoke is detected, a water valve switch is turned off. From among the 11 market apps, 6 were detected with a 100% violation ratio, both when verified independently and in conjunction with other apps; they were thus attributed as bad apps. The remaining were attributed to cause violations (with 70% or lower violation ratio) due to bad configurations (there existed safe configurations with no violations).

10.3 Violation Attribution

IoTSan attributes all of the ContextIoT’s malicious apps [51] correctly when each is independently considered with violation ratios of 100% (recall §9). Two apps violated the information leakage property as the command httpPost was executed. Two apps violated the “using security-sensitive command property”, i.e., they generated fake carbon monoxide detection events and an unsubscribe is executed. The remaining 5 apps violated safety properties in the physical space, e.g., “a main door is unlocked when no one is at home and, when smoke is detected, a water valve switch is turned off. From among the 11 market apps, 6 were detected with a 100% violation ratio, both when verified independently and in conjunction with other apps; they were thus attributed as bad apps. The remaining were attributed to cause violations (with 70% or lower violation ratio) due to bad configurations (there existed safe configurations with no violations).

10.4 Scalability

Table 7a shows the scalability benefits of our app dependency analyzer in the above experiments with 150 market apps. In this table, “Original Size” is the total number of event handlers of a group and “New Size” is the number of event handlers of the largest related set after running the App Dependency Analyzer module. On average, App Dependency Analyzer reduced the problem size by a factor 3.4x.

10.5 Concurrent vs. Sequential

Model checkers using both concurrent and sequential design detected all violations within 1 second. Table 7b shows the runtimes of the two models with a good group of apps (2 apps and 7 devices), which does not violate any property. We see that sequential design significantly reduces the runtime of the verification. Note that forever means the experiment ran for a week and then was forced to stop. Moreover, we also verified the runtime of our sequential approach with a much bigger system, which comprises of 5 related apps and 10 devices and does not have any violation. As shown in Table 8, the verification time for 10 events is about 5 hours, which is quite reasonable for a laptop with limited computing resources.

11 DISCUSSION

Application to other IoT Platforms: For ease of exposition, our narrative integrated some aspects of implementation specific to SmartThings, when describing the design of IoTSan. Conceptually, the design of IoTSan applies to other IoT platforms. To illustrate, given its recent popularity we choose IFTTT (If This Then That [46]) [55, 62, 84] to show that this is the case. IFTTT is a task automation platform for IoT deployments. An IFTTT rule (also called applet) comprises of two main parts: “Trigger Service” (This) and “Action Service” (That). To apply IoTSan to IFTTT, most of the modules (i.e., App Dependency Analyzer, Model Generator, and Output Analyzer) can be reused almost as is; the relatively big change will be in the Translator.

IFTTT to Java Translator: We use the crawler of [62] to fetch the published applets from IFTTT website into a json file. We then developed an IFTTT Handler in Java based on the org.json.simple package to extract the subscribed device and event from the trigger service, and the controlled device and expected command from
Table 5: Verification results with market apps.

<table>
<thead>
<tr>
<th>Violation type</th>
<th>Number of violations</th>
<th>Example violated property</th>
<th>Apps related to example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicting commands</td>
<td>8</td>
<td>A light receives 'on' and 'off' simultaneously</td>
<td>(Brighten Dark Places, Let There Be Dark)</td>
</tr>
<tr>
<td>Repeated commands</td>
<td>10</td>
<td>A light receives repeated 'on' commands</td>
<td>(Automated light, Brighten My Path)</td>
</tr>
<tr>
<td>Unsafe physical states</td>
<td>20</td>
<td>A heater is turned off at night when temperature is below a predefined threshold</td>
<td>(Energy Saver)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The main door is unlocked when people are sleeping at night</td>
<td>(Light Follows Me, Light Off When Close, GoodNight, Unlock Door)</td>
</tr>
</tbody>
</table>

Table 6: Verification results with market apps, with volunteer configuration.

<table>
<thead>
<tr>
<th>Violation type</th>
<th>Number of violated properties</th>
<th>Number of violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicting commands</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Repeated commands</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Unsafe physical states</td>
<td>8</td>
<td>66</td>
</tr>
</tbody>
</table>

Table 7: (a) Scalability with dependency graphs. (b) Run-times with concurrent and sequential design.

(a)  

<table>
<thead>
<tr>
<th>Group</th>
<th>Original Size</th>
<th>New Size</th>
<th>Scale Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>37</td>
<td>11</td>
<td>3.4</td>
</tr>
<tr>
<td>2</td>
<td>27</td>
<td>5</td>
<td>5.4</td>
</tr>
<tr>
<td>3</td>
<td>34</td>
<td>23</td>
<td>1.5</td>
</tr>
<tr>
<td>4</td>
<td>30</td>
<td>12</td>
<td>2.5</td>
</tr>
<tr>
<td>5</td>
<td>42</td>
<td>19</td>
<td>2.2</td>
</tr>
<tr>
<td>6</td>
<td>34</td>
<td>6</td>
<td>5.7</td>
</tr>
<tr>
<td>Mean scale ratio</td>
<td>3.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b)  

<table>
<thead>
<tr>
<th>Number of events</th>
<th>Concurrent</th>
<th>Sequential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1s</td>
<td>1s</td>
</tr>
<tr>
<td>2</td>
<td>50.3s</td>
<td>1s</td>
</tr>
<tr>
<td>3</td>
<td>139s</td>
<td>1s</td>
</tr>
<tr>
<td>4</td>
<td>forever</td>
<td>1s</td>
</tr>
<tr>
<td>5</td>
<td>4.2s</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>42.6s</td>
<td></td>
</tr>
<tr>
<td>Mean scale ratio</td>
<td>16.3s</td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Verification time vs. number of events.

<table>
<thead>
<tr>
<th>Number of events</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification time</td>
<td>6.64s</td>
<td>50.9s</td>
<td>396s</td>
<td>49.83m</td>
<td>5.89h</td>
<td>23.99h</td>
</tr>
</tbody>
</table>

by clicking on the rule), we find 7 violations of 4 unsafe physical states.

Limitations: While our prototype of IotSan has been shown to be very effective in identifying bad apps and unsafe configurations, it has the following limitations. First, the SPIN model checker has a predefined threshold for the size of Promela code (and cannot handle a file size greater than this). Depending on apps’ source code sizes and dependencies among the apps, IotSan can handle a system with about 30 apps. We assume that users are unlikely to have many more than this today and will investigate further scalability in the future. Second, we require smart apps to explicitly subscribe to specific devices they want to control and cannot handle smart apps that dynamically discover devices and interact with them. Such apps are very dangerous since they can control any device without permissions from users. Identifying such apps and ensuring that they do not compromise the physical state is beyond the scope of this effort. Third, in Algorithm 1, we let the model checker enumerate all possible permutations of the event types; thus, it may consider scenarios that are unlikely to happen in the real world (e.g., the temperature is set to a minimum value in the first iteration and set to a maximum value in the second one). However, we include these scenarios to catch bad or malicious apps. If such scenarios can be eliminated, the state explosion issue can be further mitigated. Fourth, we do not explicitly model the behavior of the physical environment after an actuator executes a command (e.g., the system temperature should increase after a heater is turned on). However, such physical changes are implicitly covered by the way the model checker exhaustively verifies a system. Fifth, the G2J Translator currently does not support heterogeneous collections (e.g., a list, array, or map that stores entries of different types) and dynamic features (e.g., overloading operator and generic data types). Note that most of the SmartThings apps do not use these features.

12 RELATED WORK

IoT Security: Current research on IoT security can be roughly divided into three categories that focus on devices [30, 39, 71], protocols [31, 40, 57, 70], and platforms. There have been efforts addressing information leakage and privacy [7, 11, 13, 74, 89, 91], and vulnerabilities of firmware images [21]. Fernandes et al., have recently reported security-critical design flaws in the IoT permission...
model that could expose smart home users to significant harm such as break-ins [27]. To address these, several efforts [28, 51, 83, 87] have proposed modifications to a smart app’s source code and the platform, to enforce good behaviors of smart apps at run time. In contrast, our work statically identifies possible violations of given physical/cyber safety properties of IoT systems without requiring any app modifications.

**Model Checking:** Model checking has been used to verify system-level threats [65–67] and basic correctness properties [14, 22, 55, 68] of IoT systems. In contrast with these efforts, IoTSan targets developing a practical platform for ensuring the physical safety of today’s IoT systems. It not only addresses the practical challenges (e.g., scale issues and making Groovy amenable to model checking) in identifying configurations that violate user properties relating to the physical state, but also addresses robustness (failures) and security issues (malicious app attribution). Table 1 shows what IoTSan offers compared to the most related recent systems.

### 13 CONCLUSIONS

Badly designed apps, undesirable interactions between installed apps and/or device/communication failures can cause an IoT system to transition into bad states. In this paper, we design and prototype a framework IoTSan that uses model checking as a basic building block to identify causes for bad physical/cyber states and provides counter-examples to exemplify these causes. IoTSan addresses practical challenges such as alleviating state space explosion with model checking, and automatic translation of app code into a form amenable for model checking. Our evaluations show that IoTSan identifies many (sometimes complex) unsafe configurations, and flags considered bad apps with 100% accuracy.

### ACKNOWLEDGMENT

We thank our shepherd Cole Schlesinger and the anonymous reviewers for their constructive comments which helped us significantly improve the paper.

The effort described in this article was partially sponsored by the U.S. Army Research Laboratory Cyber Security Collaborative Research Alliance under Cooperative Agreement W911NF-13-2-0045. The views and conclusions contained in this document are those of the authors, and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory, or the U.S. Government. The U.S. Government is not responsible for the content of any such public or private communications.

### REFERENCES


