Finding Broken Linux Configuration Specifications by Statically Analyzing the Kconfig Language

Jeho Oh∗
University of Texas at Austin
Austin, TX, USA
jeho.oh@utexas.edu

Jeho Oh∗
University of Texas at Austin
Austin, TX, USA
jeho.oh@utexas.edu

Necip Fazıl Yıldıran∗
University of Central Florida
Orlando, FL, USA
yildiran@knights.ucf.edu

Julian Braha
University of Central Florida
Orlando, FL, USA
julianbraha@knights.ucf.edu

Paul Gazzillo
University of Central Florida
Orlando, FL, USA
paul.gazzillo@ucf.edu

ABSTRACT
Highly-configurable software underpins much of our computing infrastructure. It enables extensive reuse, but opens the door to broken configuration specifications. The configuration specification language, Kconfig, is designed to prevent invalid configurations of the Linux kernel from being built. However, the astronomical size of the configuration space for Linux makes finding specification bugs difficult by hand or with random testing. In this paper, we introduce a software model checking framework for building Kconfig static analysis tools. We develop a formal semantics of the Kconfig language and implement the semantics in a symbolic evaluator called kclause that models Kconfig behavior as logical formulas. We then design and implement a bug finder, called kismet, that takes kclause models and leverages automated theorem proving to find unmet dependency bugs. kismet is evaluated for its precision, performance, and impact on kernel development for a recent version of Linux, which has over 140,000 lines of Kconfig across 28 architecture-specific specifications. Our evaluation finds 781 bugs (151 when considering sharing among Kconfig specifications) with 100% precision, spending between 37 and 90 minutes for each Kconfig specification, although it misses some bugs due to underapproximation. Compared to random testing, kismet finds substantially more true positive bugs in a fraction of the time.

CCS CONCEPTS
• Software and its engineering → Software configuration management and version control systems; Automated static analysis: Software testing and debugging.

KEYWORDS
software configuration, Kconfig, formal verification, static analysis

∗Co-first authors.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ESEC/FSE ’21, August 23–28, 2021, Athens, Greece
© 2021 Copyright held by the owner/authors(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8562-6/21/08 ... $15.00
https://doi.org/10.1145/3468264.3468578

1 INTRODUCTION
Highly-configurable software product lines underpin much of our computing infrastructure, because configurability enables reuse without having to reprogram the software for new devices or applications. The Linux kernel is one such example of highly-configurable software that is used in billions of computing devices. With over 15,000 configuration options controlling everything from drivers, architecture, memory management, and more, there are over 215,000 combinations, if only considering Boolean options. This extreme configurability makes its widespread use possible, but also opens the door to invalid configurations, which produce broken variations of the software.

To mitigate the chance of misconfiguration, developers provide configuration specifications, which define the intended combinations of configuration options. These specifications may be as simple as a text file describing configuration instructions, or as sophisticated as a machine-readable specification enforced at build time. These specifications, if only implicitly, define a software product line’s feature model, i.e., the legal configurations of the software. In Linux and other systems software, such as BusyBox and coreboot, developers use the Kconfig language to specify configuration options, as well as their dependencies.

While Linux is effectively a software product line, its specification language, Kconfig, is unlike typical feature modeling languages [47]. Kconfig has complex semantics and additional language features, such as invisible variables, automated option selection, and user-interface support. With over 140,000 lines of Kconfig specifications in the Linux kernel, its complex behavior makes maintenance challenging. One example is the common pitfall highlighted in Kconfig’s manual [28], the unmet dependency bug. These bugs lead to illegal configurations when developers unwittingly mix conflicting constructs in dependency specifications. With thousands of potentially vulnerable constructs and an ever-changing
We implement the bug-finder and evaluate it on a recent version of the Linux kernel source, which contains over 140,000 lines of Kconfig describing 28 architecture-specific Kconfig specifications. Our results show that our bug finding is both precise and fast. The bug-finder finds 781 alarms (151 when considering sharing among Kconfig specifications) over all Linux kernel architectures’ Kconfig specifications, all of which are verified true positives, for a precision of 100%. While such precision might be unusually high for a programming language analyzer, the Kconfig language has no iteration or recursion that would require overapproximation. With our optimizations, our bug finder takes an average of 40 minutes for one Kconfig specification, checking over 10,000 constructs.

While we are still in the process of reporting all bugs found by our tool, Linux maintainers have so far already confirmed 38 of our reports and committed 15 of our patches into the mainline Linux kernel repository, demonstrating the utility of our tooling. Committing patches is a manual process, requiring discussion with kernel maintainers, so investigating, reporting, and submitting patches for the alarms is ongoing.

Since, to our knowledge, no other static bug finder for unmet dependencies exists, we compare to Kconfig’s built-in randconfig tool, the de facto standard random configuration testing tool used by Linux maintainers and the Intel 0-day test service [5]. Given the same amount of time to find bugs, randconfig yields only 98 alarms compared to our tool’s 781. Even letting random testing run for over four days for each Kconfig specification, 135x longer than our tool’s total time, the testing approach still only finds 175 bugs, far fewer than our tool. The random testing approach did find eight bugs missed by our tool, reflecting the tradeoff in performance gained by underapproximation. Even with this limitation, our tool finds many more bugs while taking far less time, a useful complement to testing.

In summary, this paper makes the following contributions:

- A formal semantics of Kconfig’s concrete behavior (Section 3).
- An efficient design of a bug-finder and localizer for unmet dependency bugs (Section 4).
- An implementation of the bug finder, along with reusable components for creating Kconfig analyzers (Section 5).
- An experimental evaluation of the bug finder’s precision, performance, and impact (Section 6).

2 OVERVIEW

In this section we introduce the Kconfig language, illustrate an unmet dependency bug, and summarize how our formal semantics enables the design of a static analysis to find such bugs.

2.1 Introduction to the Kconfig Language

Figure 1 is a simplified snippet of Kconfig from Linux v5.4.4. Configuration options are defined with the config construct (lines 1, 7, and 12). Inside each config declaration is a block of constructs that define the option’s type (e.g. Boolean), constraints on its use, and text used by Kconfig to populate a user interface.

Lines 2, 8, and 13 are the type declarations. A bool option (line 8) has two possible settings, y or n. y means the feature is on and compiled into the kernel, and n means the feature is off and omitted.
An Unmet Dependency Bug in the Wild. Figure 1 has an unmet dependency bug found by our automated analysis. All three of the configuration options defined in this example control specific C compilation units that are only built into the kernel when the options are enabled. IIO_BUFFER_CB controls industrialio-buffer-cb.o and IIO_BUFFER_CB controls industrialio-buffer.o. industrialio-buffer-cb.o calls functions that are defined in industrialio-buffer.o, so the former cannot be built without the latter, otherwise there would be a build error. The developers capture this build dependency with a direct dependency in the definition of the IIO_BUFFER_CB option (line 15). This constraint, by itself, would prevent a user from giving a configuration that leads to the build error.

The select IIO_BUFFER_CB construct on line 5, however, can override this direct dependency under certain conditions. Specifically, if a user (or another select) enables TOUCHSCREEN_ADC, the select automatically force-enables IIO_BUFFER_CB. Kconfig permits such a configuration to proceed to build, albeit with a warning. Still, the build will fail, and the user will have to manually correct their configuration file in order to avoid the unmet dependency.

While the Kconfig documentation warns of select’s pitfalls and recommends not using it to override dependencies, it is difficult to check by hand whether any of its 17,000+ uses have an unmet dependency bug.

2.2 An Unmet Dependencies Bug Finder

We create a formal model of the unmet dependency bug according to the semantics of Kconfig. First, we model the space of valid Kconfig configurations in formal logic automatically with our symbolic evaluator kclause. Next, kismet generates verification conditions to prove the absence of an unmet dependency for each select construct in the Kconfig specification. Not all reverse dependencies can cause unmet dependencies, so kismet needs to consider constraints from all configuration options to rule out infeasible ones. The resulting verification conditions are discharged to the Z3 SMT solver [13]. When an unmet dependency cannot be ruled out, kismet raises an alarm. It then switches to test case generation, converting any counterexamples to Linux configuration files. kismet uses these tests on Kconfig and the build system to expose real bugs.

To see how kclause models dependencies, take Figure 1’s definition of TOUCHSCREEN_ADC (line 1). Since it has no reverse dependencies, it can only be enabled when its direct dependencies hold, i.e., enabling TOUCHSCREEN_ADC implies IIO and INPUT_TOUCHSCREEN are also enabled:

TOUCHSCREEN_ADC \rightarrow IIO \land INPUT_TOUCHSCREEN

When an option has reverse dependencies, its direct dependencies do not have to hold if its reverse dependencies already do. For instance, enabling IIO_BUFFER_CB (line 12) implies that its direct or reverse dependencies hold:

\begin{align*}
IIO_BUFFER_CB \rightarrow & (IIO \land IIO_BUFFER \\
& \lor TOUCHSCREEN_ADC)
\end{align*}

An unmet dependency happens when an option’s reverse dependencies hold but its direct dependencies do not. For instance, an unmet dependency happens when TOUCHSCREEN_ADC force-enables
The Kconfig language is a declarative configuration specification even though IIO_BUFFER_CB for reverse dependencies. Constraints for direct dependencies, and zero or more or a choice construct. A configuration option, has a type, constraints for direct dependencies, and zero or more select constructs for reverse dependencies.

3 THE SEMANTICS OF KCONFIG

The Kconfig language is a declarative configuration specification language. At its core, Kconfig takes a configuration file, which is a mapping from configuration options to their concrete values, and determines whether the configuration file is valid according to the developer’s specifications. Developers use Kconfig language constructs to define configuration options, declaring their names, types, and any dependencies they have on other configuration options. Kconfig also supports user interfaces, and the language has additional constructs, such as help, to specify text elements of the interface. These do not affect the buildability of configuration files and act as comments.

We developed this formal semantics by studying the Kconfig manual, Kconfig’s source code, as well as informal descriptions and examples from prior work [15, 16]. To check the fidelity of the semantics, we used new and existing benchmarks [15, 16], generated random configuration files fed to Kconfig as input, and evaluated this paper’s bug-finder, which requires a correct semantics for its analysis to be precise. Given the size of the semantics, having dozens of rules and still more syntactic sugar rules, we highlight a core fragment of the language here, and document the remaining rules in an openly-archived formal semantics [40].

3.1 Configuration Declarations

Figure 2 shows the syntax of a core fragment of the Kconfig language for bool configuration options. A kconfig file contains a list of statements, which are either configuration option declarations or a choice construct. A configuration option, config, has a type, constraints for direct dependencies, and zero or more select constructs for reverse dependencies.

Figure 3a defines the semantic valuation function S for statements. S functions take an immutable configuration file σ as input and return whether the configuration is valid or invalid, i.e., buildable or not. S1 evaluates a Kconfig specification’s list of statements by checking whether all statements are valid according to the input.

S2 is the valuation function for config statements. The number of cases reflects the complexities of Kconfig’s validity checking. The first covers reverse dependencies, using the valuation function R, which searches the entire kconfig file. (In practice, the Kconfig implementation memoizes reverse dependencies during parsing to avoid repeatedly traversing the syntax tree.) If a reverse dependency holds, that means the option must be enabled, i.e., σ(sym) = y, otherwise the configuration file does not match the specification.

The second case of S2 handles a direct dependency when the reverse dependency does not hold. In this case, an option is valid regardless of its setting, because a user is free to enable or disable it. The third case covers non-visible configuration options, which have no prompt, so the option’s value must match the specified default. The fourth case covers when none of the option’s dependencies hold. Lastly, if none of these conditions are met, the configuration file is not valid.

Dependencies for non-Boolean types (string, int, and hex) behave similarly to bool and tristate, but there are additional constraints and expressions such as range and inequalities. The full semantics describes these differences [40].

3.2 Reverse Dependencies

To find any reverse dependencies for an option, Kconfig needs to search the entire specification for a select that can enable the option. This is partly why tracking down unmet dependencies is so difficult.

Figure 3b defines the valuation function R for reverse dependencies. It takes both the configuration file σ and a symbol name s and returns a Boolean value: true if that symbol is selected by some option or false if not. R1’s disjunction reflects the need for only one select to force-enable an option.

R2 checks to see if an option is enabled and its dependencies are met, then calls R3 to evaluate any select constructs. R3 checks whether there is a select for the input symbol s. R4 checks whether any configuration option within a choice block selects symbol s.

Options other than tristate and bool cannot be the selector or selectee of a reverse dependency.

3.3 Choice Constructs

A choice construct defines a mutually-exclusive set of configuration options. Choices are useful in configuration specifications, because expressing them with Boolean logic alone is verbose. Figure 4 is an example of a choice from the Linux kernel that allows only one of several compression algorithms for a file system to be enabled. A choice block starts with a choice keyword (line 1) and ends with an endchoice (line 10). It contains a list of configuration options which, besides the mutual-exclusion rule, behave mostly like any other options, except that they cannot have reverse dependencies or default values.
Finding Broken Linux Configuration Specifications by Statically Analyzing the Kconfig Language

ESEC/FSE ’21, August 23–28, 2021, Athens, Greece

\[(S_1)\quad S[[kconfig]]_\sigma^A \triangleq \begin{cases} \text{valid} & \text{if } \wedge_{\text{statement}_i \in \text{kconfig}} (S[[\text{statement}_i]])_\sigma = \text{valid} \\ \text{invalid} & \text{otherwise} \end{cases} \]

\[(S_2)\quad S[[\text{config sym bool constrnts select*}]]_\sigma^A \triangleq \begin{cases} \text{valid} & \text{if } (\sigma(\text{sym}) = y) \wedge R[[\text{kconfig}]](\sigma, \text{sym}) \\ \text{invalid} & \text{otherwise} \end{cases} \]

\[(S_3)\quad S[[\text{choice bool constrnts config+ end}]]_\sigma^A \triangleq \begin{cases} \text{valid} & \text{if } (\text{Enabled}[[\text{config+}]]_\sigma = 1) \wedge (S[[\text{config+}]]_\sigma = \text{valid}) \\ \text{invalid} & \text{otherwise} \end{cases} \]

(a) Direct dependency rules.

\[(R_1)\quad R[[\text{kconfig}]](\sigma, s) \triangleq \bigvee_{\text{statement}_i \in \text{kconfig}} R[[\text{statement}_i]](\sigma, s) \]

\[(R_2)\quad R[[\text{config sym bool constrnts select*}]](\sigma, s) \triangleq \begin{cases} R[[\text{select*}]](\sigma, s) & \text{if } (\sigma(\text{sym}) = y) \wedge E[[\text{depends+}]](\sigma) \\ \text{false} & \text{otherwise} \end{cases} \]

\[(R_3)\quad R[[\text{select} sym if expr select*]](\sigma, s) \triangleq \begin{cases} R[[\text{select*}]](\sigma, s) & \text{if select* } \neq \emptyset \\ \text{false} & \text{otherwise} \end{cases} \]

\[(R_4)\quad R[[\text{choice bool constrnts config+ end}]](\sigma, s) \triangleq \begin{cases} R[[\text{config+}]](\sigma, s) & \text{if } E[[\text{depends+}]](\sigma) \wedge E[[\text{prompt}]](\sigma) \\ \text{false} & \text{otherwise} \end{cases} \]

(b) Reverse dependency rules.

\[\Sigma : \text{Symbols} \rightarrow \{y, n\} \]
\[S : \text{Statements} \rightarrow (\Sigma \rightarrow \{\text{valid, invalid}\}) \]
\[R : \text{Statements} \rightarrow (\Sigma \times \text{Symbols} \rightarrow \{\text{true, false}\}) \]
\[E : \text{Constraints} \rightarrow (\Sigma \rightarrow \{\text{true, false}\}) \]

(c) Types for input (\Sigma) and the valuation functions.

\[\text{Enabled}[[\text{config+}]]_\sigma \triangleq \sum_{\text{sym} \in \text{config+} \atop \sigma(\text{sym}) = y} (1) \]

(d) Counting how many config options are enabled.

\[(E_1)\quad E[[\text{prompt word if expr}]]_\sigma^A \triangleq E[[\text{expr}]](\sigma) \]

\[(E_2)\quad E[[\text{depends+}]]_\sigma^A \triangleq \bigwedge \{E[[\text{expr}_{i+}]]_\sigma \atop \text{expr}_{i+} \in \text{depends+}\} \]

\[(E_3)\quad E[[\text{default val if expr default}]]_\sigma^A \triangleq \begin{cases} E[[\text{default*}]](\sigma) & \text{if default* } \neq \emptyset \\ \text{false} & \text{otherwise} \end{cases} \]

\[(E_4)\quad E[[\text{expr}_{i} \&\& \text{expr}_{j}]]_\sigma^A \triangleq E[[\text{expr}_{i}]]_\sigma \wedge E[[\text{expr}_{j}]]_\sigma \]

\[(E_5)\quad E[[\text{expr}_{i} || \text{expr}_{j}]]_\sigma^A \triangleq E[[\text{expr}_{i}]]_\sigma \vee E[[\text{expr}_{j}]]_\sigma \]

\[(E_6)\quad E[[\text{! expr}]]_\sigma^A \triangleq \neg E[[\text{expr}]]_\sigma \]

\[(E_7)\quad E[[\text{sym}]]_\sigma^A \triangleq (\sigma(\text{sym}) = y) \]

(e) Expression evaluation rules.

Figure 3: Formal semantics of a core fragment of Kconfig.
The menu sugars rules needed. defines ordering on constraints to reduce the number of syntactic syntax. Most of the behavior of a Kconfig specification is insensitive to the ordering of options and constraints. Therefore, our syntax defines ordering on constraints to reduce the number of syntactic sugars rules needed.

### 3.4 Constraint Expressions

Figure 3e defines rules for evaluating constraint expressions, which return a Boolean true or false. \( E_1, E_2, \) and \( E_3 \) are the prompt, \( \text{depends on} \), and \( \text{default} \) constructs, respectively. Each is a carrier for a logical expression, and it is their interaction with \( \text{config} \) and \( \text{choice} \) that gives them distinct meaning. The rest of the rules are typical Boolean operators \( (E_4, E_7) \).

### 3.5 Syntactic Sugar

Kconfig has three additional statements that can be desugared to \( \text{config} \) and \( \text{choice} \): if, menu, and menuconfig. Unlike the control-flow construct in programming languages, Kconfig’s if is just syntactic sugar for adding constraints in bulk to its nested statements. The menu statement behaves like an if block, but also adds text to the user interface. menuconfig is a combination of config and menu. The full semantics [40] contains the desugaring rules for these.

The Kconfig language also has a great deal of flexibility in its syntax. Most of the behavior of a Kconfig specification is insensitive to the ordering of options and constraints. Therefore, our syntax defines ordering on constraints to reduce the number of syntactic sugars rules needed.

```plaintext
1 choice
2  prompt "Decompressor parallelisation options"
3  depends on SQUASHFS
4 config SQUASHFS_DECOMP_SINGLE
5    bool "Single threaded compression"
6 config SQUASHFS_DECOMP_MULTI
7  bool "Use multiple decompressors"
8 config SQUASHFS_DECOMP_MULTI_PERCPU
9    bool "Use percpu multiple decompressors"
10 endchoice
```

**Figure 4:** An example of a choice construct.

The \( S_3 \) function in Figure 3a describes the choice block’s semantics. The first case covers the mutual exclusion property, requiring that only one of the configuration options is enabled. This condition also recursively checks that all the nested configs’ dependencies are valid.

Choice constructs also have their own direct dependencies, so Kconfig permits no options to be enabled when the choice dependencies are not met. The second case of \( S_3 \) covers this situation. The third case covers the situation when none of the nested config options’ dependencies are met, in which case Kconfig also permits the choice to have no options enabled. choice constructs can also take the optional keyword to allow for no options to be enabled even if its direct dependencies are met. The rules are slightly different from a regular choice, and we present them in the full semantics [40].

The choice statement described above has bool type. The only other type a choice can take is tristate, in which case its behavior is the same as bool, except that more than one choice may be set to \( m \).

### 4 DESIGNING THE BUG FINDER

Kconfig has limited metaprogramming facilities via preprocessor constructs for file inclusion and macro expansion [2], which we do not model. Our implementation runs the preprocessor before symbolic evaluation to ensure that all files are included and macros are expanded.

#### 4.1 Identifying Select Constructs

Kconfig identifies select constructs, as well as semantic analysis, to construct a formal model of the bug automatically. kismet discharges the formal conditions to an SMT solver to check satisfiability. The Kconfig language allows developers to define constraints using symbolic Boolean formulas. Since our goal is to analyze all solutions to these constraints simultaneously, the analysis problem is at least as hard as Boolean satisfiability in general. The main challenge to designing kismet is ensuring scalability while preserving enough precision to identify the exact constructs causing the unmet dependency alarm.

The schematic in Figure 5 highlights what conditions kismet identifies as the configurations under which it triggers an unmet dependency bug. This requires both syntax analysis, to identify select constructs, as well as semantic analysis, to construct a formal model of the bug automatically. kismet discharges the formal conditions to an SMT solver to check satisfiability. The Kconfig language allows developers to define constraints using symbolic Boolean formulas. Since our goal is to analyze all solutions to these constraints simultaneously, the analysis problem is at least as hard as Boolean satisfiability in general. The main challenge to designing kismet is ensuring scalability while preserving enough precision to identify the exact constructs causing the unmet dependency alarm.

```plaintext
1 config X
2  select A if DX
3    K_X // other constraints for X
4 config A
5  depends on DA
6    K_A // other constraints for A
7 K_Other // constraints from other configuration options
```

**Figure 5:** Components of an unmet dependency condition.
4.2 Modeling Unmet Dependency Bugs

X’s select construct only causes an unmet dependency if the select overrides A’s direct dependencies, i.e., when A’s dependencies are unsatisfied. If we just consider the constraints of the selector and the selectee, the formula for unmet dependency is as follows:

\[ \phi_{\text{unmet}} = X \land D_X \land K_X \land A \land \neg(D_A \land K_A) \quad (1) \]

\[ \phi_{\text{unmet}} \text{ means the following: the selector option } X \text{ is enabled and its select and other constraints } D_X \land K_X \text{ are met (subexpression 1); and the selectee option } A \text{ is enabled while its dependencies } D_A \land K_A \text{ are not met (subexpression 2).} \]

\[ \phi_{\text{unmet}} \text{ is an overapproximation, however, because it only accounts for the constraints from two configuration options, the selector and selectee. Constraints from other configuration options } (K_{\text{other}}) \text{ can make } \phi_{\text{unmet}} \text{ unsatisfiable. Without accounting for those, we can expect more false positive alarms. A precise condition would contain these constraints as well:} \]

\[ \phi_{\text{unmet (precise)}} = \phi_{\text{unmet}} \land K_{\text{other}} \]

Optimizing the bug-finder. The Linux Kconfig specification has thousands of configuration options, so \( \phi_{\text{unmet (precise)}} \) is a substantially more expensive formula to solve; it has the constraints from thousands of configuration options instead of just the two in \( \phi_{\text{unmet}} \). To make solving more efficient, we use two techniques. First, if a selectee option has no direct dependencies, then an unmet dependency bug is not possible. Second, we first check the \( \phi_{\text{unmet}} \) condition and only check \( \phi_{\text{unmet (precise)}} \) if the first check is satisfiable. This optimization is safe, because if \( \phi_{\text{unmet}} \) is unsatisfiable, we know that \( \phi_{\text{unmet (precise)}} \) is also unsatisfiable, i.e., \( \neg \phi_{\text{unmet (precise)}} \) entails \( \neg \phi_{\text{unmet}} \): \( \phi_{\text{unmet}} \rightarrow \phi_{\text{unmet (precise)}} \) tautology

\( \phi_{\text{unmet (precise)}} \rightarrow \phi_{\text{unmet (precise)}} \) strengthening

\( \phi_{\text{unmet}} \land K_{\text{other}} \rightarrow \phi_{\text{unmet (precise)}} \) substitution

\( \neg \phi_{\text{unmet}} \rightarrow \neg \phi_{\text{unmet (precise)}} \) contraposition

This simple optimization has a substantial impact on precision and performance as we show in the evaluation section.

4.3 Modeling Kconfig Semantics

Until now, we have described \( \phi_{\text{unmet}} \) with placeholders for configuration option constraints. But interpreting these constraints as logical formulas requires modeling Kconfig’s semantics. In this section we show how we methodically derive these from our formal semantics (Section 3).

Recall that Kconfig takes a configuration file as input and determines its validity according to the specifications. As with prior Kconfig feature modeling tools, we represent configuration options as symbolic Boolean options, collapsing tristate option’s y and m to true. While this underapproximates tristate, it greatly reduces the space of possible configurations, improving solver performance. Similarly, we approximate non-Booleans with a finite range of options, as in prior work [30]. Less than 5% of options are non-Boolean in Linux Kconfig specifications.

To derive the model from Kconfig semantics, recall that our concrete semantics describes each case in which a Kconfig statement describes a valid configuration given an input configuration file. For each Kconfig syntactic construct in the specification under analysis, our bug finder automatically constructs a symbolic formula \( \phi_i \) corresponding to its valuation function from the semantics in Figure 3. The formula is the disjunction of each condition leading to a valid result. For instance, a config statement, defined by semantic rule \( S_2 \) in Figure 3, has four valid cases. 

\[
\phi_{\text{config}} = (C \land \phi_{\text{reverse}}) \\
\lor (\phi_{\text{depends}} \land \phi_{\text{prompt}} \land \neg \phi_{\text{reverse}}) \\
\lor (C \land \phi_{\text{default}} \lor \neg C \land \neg \phi_{\text{default}}) \\
\lor (\neg C \land \neg \phi_{\text{prompt}} \land \neg \phi_{\text{reverse}})
\]

Each of the four disjunctive terms corresponds to each of the four valid conditions from \( S_2 \). Accesses to the concrete configuration option value \( \sigma \text{(sym)} \) are replaced with a symbolic Boolean value \( C \). Calls to other valuation functions are replaced with the symbolic formulas for that syntax, e.g., \( \phi_{\text{depends}} \) for the depends on construct.

For the configuration option IIO_BUFFER_CB in Figure 1, \( \phi_{\text{config}} \) is constructed from the following symbolic formulas:

\( C = IIO\_BUFFER\_CB \)

\( \phi_{\text{reverse}} = \text{TOUCHSCREEN\_ADC} \land \text{IIO} \land \text{INPUT\_TOUCHSCREEN} \)

\( \phi_{\text{depends}} = \text{IIO} \land \text{IIO\_BUFFER} \)

\( \phi_{\text{prompt}} = \text{true} \)

\( \phi_{\text{default}} = \text{false} \)

\( \phi_{\text{reverse}} \) and \( \phi_{\text{direct}} \) are the reverse and direct dependencies respectively. The option is always visible since it has an unconditional prompt \( \phi_{\text{prompt}} \), and the default value is false since it has no default specification \( \phi_{\text{default}} \).

Substituting the symbolic formulas into \( \phi_{\text{config}} \) and simplifying the disjunctive terms, we get the following:

\[
(IIO\_BUFFER\_CB) \\
\land \text{TOUCHSCREEN\_ADC} \land IIO \land \text{INPUT\_TOUCHSCREEN}) 
\lor (IIO \land IIO\_BUFFER) \\
\land (\neg(\text{TOUCHSCREEN\_ADC} \land IIO \land \text{INPUT\_TOUCHSCREEN})) 
\lor (\neg(IIO\_BUFFER\_CB) \land \neg(IIO \land IIO\_BUFFER)) \\
\lor (\neg(\text{TOUCHSCREEN\_ADC} \land IIO \land \text{INPUT\_TOUCHSCREEN}))
\]

In summary, this formula means that IIO_BUFFER_CB is legal to enable if its reverse dependency holds (subexpression 3), is legal to either enable or disable if its direct dependency holds (subexpression 4), never takes a default value (subexpression 5), and can otherwise only be disabled when its direct and reverse dependencies do not hold (subexpression 6). The rest of the symbolic evaluator’s valuation functions are similarly derived from the formal semantics and can be found with the openly-archived formal semantics [40].

The benefit of this approach is that it removes guesswork from designing Kconfig analysis tools. Instead, tool writers can rely on a common semantics to mechanically derive an analysis for whatever abstraction they would like to use for analysis, tailoring the choice of formalism for configuration options based on their specific application. We demonstrate just one possible set of choices for deriving
5 IMPLEMENTATION

The analysis framework is implemented in about two thousand source lines of Python, and about one thousand source lines of C. It consists of four components, shown in Figure 6. The kextract tool wraps the parser from the Linux implementation of Kconfig [54] with a C extension to desugar the Kconfig specification into a desugared version of the Kconfig language. The kclause tool, written in Python, reads in desugared Kconfig and constructs logical formulas for each configuration options’ constraints, outputting them in the SMTLIB2 [9] format. kismet, also written in Python, finds each select construct from the kextract output and uses the logical models from kclause to generate the unmet dependency condition for each construct. kismet finally passes this condition in SMTLIB2 format to the klocalizer tool, which uses the Z3 SMT solver [13] to check for the satisfiability of the bug condition. For satisfiable conditions, klocalizer can also generate solutions to the condition in the Linux .config file format, which we use to test the solution against the actual Kconfig implementation. All source code is available online as free and open-source software1 as well as in an openly-archived artifact [38].

6 EXPERIMENTAL EVALUATION

We evaluate our bug finding approach for precision, performance, and impact on real-world code.

6.1 Experimental Setup

We use Kconfig specifications from a recent version (v5.4.4) of the Linux kernel source code2 as the target of our study. With over 140,000 lines of specifications and over 15,000 configuration options, Linux represents, to our knowledge, the largest user of Kconfig.

The Linux kernel not only provides a large Kconfig specification, but multiple ones as well, due to its support for multiple hardware platforms. Each of its 28 architecture families has its own Kconfig specification, effectively providing 28 separate Kconfig specifications to use for evaluation. Because of the hardware abstraction layer, however, these architectures share at least some portion of the codebase in common, and therefore also share a large portion of their Kconfig specifications; about 100,000 lines, two-thirds, are architecture-independent. Each architecture has between 10,014 and 12,744 select constructs for a total of 289,202. Deduplicating these, there are 17,006 unique select constructs, although the constraints due to architecture-specific Kconfig files may differ. Due to this sharing, we not only report results for each architecture’s Kconfig specifications but also the aggregate and deduplicated alarms across architectures.

All experiments were executed on a server with an AMD EPYC 7401 24-Core Processor with 512GB of RAM running Ubuntu 18.04, where we measured performance using the UNIX time utility. Since this machine allows for high parallelism, we ran the experiments for the 28 architectures’ Kconfig specifications in parallel on separate copies of the Linux kernel source code. Replication scripts are available with the source code repository3.

6.2 Data Availability

All experimental data are available as archived open data [39].

6.3 Research Questions

Our evaluation seeks to answer the following research questions:

RQ1 (Precision) How precise is our analysis when finding unmet dependencies? To measure bug-finding effectiveness, we run our tool on all 28 Linux Kconfig specifications and collect the alarms reported. We also automatically validate whether the alarms are true positives by generating and building test cases automatically. We expect that, if our semantics reflect real Kconfig behavior, our symbolic model of unmet dependencies and Kconfig behavior should yield high precision, i.e., few false positives.

RQ2 (Performance) How fast is bug-finding? We record the running time of our bug-finder when applied to all 28 Linux Kconfig specifications, i.e., the experiment from RQ1. We report the distribution of running times per architecture, the aggregate time, as well as the breakdown between desugaring, generating bug conditions, and solving. We expect that our design choices and optimization will yield a fast enough analysis to make running kismet feasible for developers to use regularly.

RQ3 (Impact) How useful are the resulting alarms to developers? We evaluate the impact of our bug-finding approach by manually submitting some reports and patches to the kernel

---

1https://github.com/paulgazz/kmax

2https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.4.4.tar.xz

3alpha, arm, arm64, cc, csky, h8300, hexagon, i386, ia64, m68k, microblaze, mips, mips32, mips64, openrisc, parisc, powepe, riscv, s390, sh, sh64, sparc, sparc64, um, unicore32, x86_64, and xen
maintainers. We expect that, if the resulting alarms are correct and provide value to the kernel maintainers, they will confirm the reports and accept our patches.

RQ4 (Comparison) How does our approach compare to random configuration testing? To our knowledge, no related tool for finding unmet dependencies in Kconfig exists. To provide a baseline time to search for bugs, we use random configuration testing with Kconfig’s built-in randconfig tool. We compare the bugs found, given the same amount of time as kismet and also allow randconfig generation to run for several days. We expect that our static approach will perform better, given the enormity of the search space of configurations, but we also expect to find new bugs missed by kismet’s underapproximation of non-Booleans.

### 6.4 RQ1: Precision

We run kismet on each of the 28 architectures’ Kconfig specifications and collect the resulting alarms. kismet reports the pair of configuration options involved in the unmet dependency, i.e., the selector and the selectee. Finally, we validate whether the alarm is a true positive by generating a test case. This works by querying the Z3 SMT solver for a satisfying solution to \( \phi_{\text{unmet}} \), the bug’s logical formula, then converting the solution into the Linux .config configuration file format.

Table 1 summarizes the analysis results of our experiments. The rows list the number of constructs analyzed, the number of alarms raised by kismet, and the precision, i.e., the percent of all alarms that are true positives. The columns show the distribution of these metrics across the 28 architectures’ Kconfig specifications as percentiles. kismet checks between 10,014 and 12,744 select constructs for each architecture, finding between 10 and 53 alarms per Kconfig specification, for a total of 781 alarms over 289,202 constructs. All alarms are confirmed to be true positives by generating test cases that trigger the alarm, for a precision of 100%. While such high precision would be unusual for static analysis, the core fragment of Kconfig that we model requires no over-approximation that could lead to false positives. Since the ground truth number of bugs in real-world Linux Kconfig specifications is unknown, we do not compute recall, but we address false negatives in RQ4.

Although each architecture has its own Kconfig specification, they all share a large common set of Kconfig files. The consequence is that fixing a bug in one architecture’s Kconfig specification can fix it for several others. Deduplicating these bug yields 151 total alarms for unique select constructs across all architectures. In some cases, the same select construct was a true unmet dependency in one architecture’s Kconfig specification but not others, which is possible because of architecture-specific constraints. In these cases, we counted the construct as a true alarm in the deduplicated set.

Summary: our approach is precise, yielding 100% precision on Linux’s very large, real-world Kconfig specification, and finds many new bugs: 781 true positive bugs or 151 if we deduplicate common constructs across architectures.

### 6.5 RQ2: Performance

To evaluate performance, we measure kismet’s running time, broken down by each phase of its analysis. Table 2 is the distribution of running times across each of the 28 architecture-specific Kconfig specifications. Each row is the phase of analysis, with the total time in the last row, while each column is percentiles in the distribution of running times.

Table 2: kismet’s bug-finding time in minutes for all 28 Kconfig specifications, broken down by each phase of analysis.

<table>
<thead>
<tr>
<th>Analysis Phase</th>
<th>Time Percentiles (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max</td>
</tr>
<tr>
<td>kclause</td>
<td>7.21</td>
</tr>
<tr>
<td>Syntax check</td>
<td>0.15</td>
</tr>
<tr>
<td>( \phi_{\text{unmet}} )</td>
<td>2.35</td>
</tr>
<tr>
<td>( \phi_{\text{unmet (precise)}} )</td>
<td>79.31</td>
</tr>
<tr>
<td>Confirmation</td>
<td>2.01</td>
</tr>
<tr>
<td>Total Time</td>
<td>90.21</td>
</tr>
</tbody>
</table>

Summary: kismet is fast, taking between 37 and 90 minutes to analyze between 10,014 to 12,744 select constructs in a Kconfig specification, enabling frequent bug finding runs.
6.6 RQ3: Impact

We evaluate the impact of our bug-finder, and the semantics on which it is based, by reporting alarms to the kernel developers and submitting patches to the mainline Linux repository, specifically via the Linux kernel mailing list [50] and the kernel.org Bugzilla website [3]. Developer confirmation of bugs provides confidence in the utility of the alarms, beyond precision. Moreover, acceptance of patches by official maintainers reflects the beneficial impact of the results on this prevalent and frequently used codebase.

While our bug-finder is fully automated, submitting reports and patches is a manual process, requiring time to create them and communicate with human Linux maintainers. Moreover, maintainers may opt to not patch even true alarms, may not respond immediately, or may request different changes than what we proposed in the patch. Since the Kconfig specification gradually changes over time with the rest of the codebase, prior bugs may no longer occur, due to manual fixes, removal of options, etc. We believe it is feasible to use kismet in continuous integration, but we leave such infrastructure development as future work. For these reasons, we have not yet submitted all alarms; repairing all is an ongoing process, and we report the current state of the bug repairs in progress.

As of writing, we have submitted 38 reports or patches, 19 have been confirmed with the remainder pending, and 15 of our patches have already been committed to the Linux kernel codebase. Up-to-date information about the reporting and patching effort can be found in the source code repository\(^4\).

Knowing the effect of unmet dependencies on the kernel is difficult to measure. Such a configuration is not supposed to be feasible, and developers have been so far highly receptive to patches of unmet dependency bugs. While we do not know all the effects of an unmet dependency, one common result is a broken build, e.g., Figure 1, which is undesirable for any software product. We measured how often a broken build results from the bugs we found by attempting to build the generated .config from kismet and hand-checking the reason for the broken build. Build errors account for 68% of all tests. 29% of configuration files trigger build errors whose root cause is the unmet dependency bug from which the configuration file was generated. 27% fail due to bugs other than the one used to generate the test case. Since a build error halts the build process, we cannot easily determine whether the build would have encountered an error related to the unmet dependency, so we conservatively assume these are not caused by unmet dependencies.

**Summary:** The bug finding results have resulted in 38 reports and 15 committed patches to the Linux kernel so far, with further patch submission and discussion ongoing.

6.7 RQ4: Comparison

While kismet is 100% precise for its fragment of the Kconfig semantics, its underapproximation of non-Boolean leaves it susceptible to false negatives. To gather a set of unmet dependency benchmarks that include bugs not findable by kismet, we use a built-in Kconfig utility for generating random configurations. Generating random configurations for over four days for each architecture in parallel (a combined time of more than three months), we generated over 11,000,000 configuration files, which raised 2,857,938 unmet dependency alarms, yielding 175 unique unmet dependency bugs. Comparing these to kismet’s results, kismet adds 614 unique unmet dependencies not found in this random testing.

Since no other tools to our knowledge analyze unmet dependencies, we compare the performance of kismet against a random testing approach, to see whether there is a benefit in running time and bugs found to using kismet. Using the combined set of bugs from months of randconfig and kismet’s results, we compare the percent of bugs found given the same amount of time. Table 3 shows the results of this comparison of the percentage of bugs found from the benchmark set. The columns show the distribution of these percentages across all architectures’ Kconfig specifications. kismet finds 100% for almost all architectures, reflecting the fact that even after months of compute time, very few additional bugs were found by random testing compared with kismet. randconfig (row “Same time”), given the same amount of time that kismet took, finds on average only a small fraction of the set of bugs, 6.80%, with a maximum of only 62.86%. Even given several days to run (row “135x time”), randconfig still only finds a fraction of the benchmark bugs. In contrast, there were only eight bugs not found by kismet, leading to a worst-case of 87.10% benchmark coverage by kismet.

While our benchmark is not the ground truth of Linux’s complete set of bugs, which is not feasible to find by hand given the months of compute time to generate configuration files, it provides at least an estimate of the relative performance of kismet versus random testing. The results show the large performance benefit of using kismet compared to random testing. In the same amount of time, kismet finds many more bugs than random testing, providing a fast and precise complement to random testing that can be run regularly against new commits to the Kconfig specification.

**Summary:** kismet finds many more true positives bugs in far less time than random testing, although there are also false negatives as expected by deliberate underapproximation.

### Table 3: Percent of the bugs found by kismet compared to randconfig given both the same amount of time as and 135x more time than kismet.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Percentiles Max</th>
<th>Percentiles 75th</th>
<th>Percentiles 50th</th>
<th>Percentiles 25th</th>
<th>Percentiles Min</th>
</tr>
</thead>
<tbody>
<tr>
<td>kismet</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>87.10%</td>
</tr>
<tr>
<td>randconfig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Same time</td>
<td>62.86%</td>
<td>12.94%</td>
<td>6.80%</td>
<td>2.68%</td>
<td>0.00%</td>
</tr>
<tr>
<td>135x time</td>
<td>77.14%</td>
<td>22.55%</td>
<td>17.42%</td>
<td>10.54%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

4https://github.com/paulgazz/kmax/blob/master/docs/bugs_found.md

7 THREATS TO VALIDITY

**Internal Threats.** Our formal semantics needs to match the actual behavior of Kconfig, otherwise, any analyses based on it may yield incorrect results. We mitigated this using the Kconfig documentation, reviewing its actual C implementation, and collecting a Kconfig test suite. Moreover, the 100% precision of the bug-finder, validated with generated test cases and some developer confirmation, testifies to the accuracy of the semantics. kismet is deliberately underapproximate for non-Boolean options, however, so this part of the
semantics is not supported by the bug-finding results, but by the documentation, implementation, and test suite only.

**External Threats.** While Kconfig is used by several popular, low-level systems software (BusyBox, coreboot, etc), our evaluation only applies to Linux. Linux, however, is the largest user of Kconfig that we know of, and has multiple Kconfig specifications. We evaluate our bug-finder on one recent version of the Linux source code, but Kconfig specifications change gradually with each kernel version. Different versions may yield different numbers of alarms. We leave a long-term study of Kconfig bugs across versions and projects as future work. Our bug-finder currently checks for one kind of bug. The performance of the bug-finder could vary for different bug types or analysis tasks. Our work is specific to the Kconfig specification language, so we do not show applicability to other specification languages. Given the large time investment in creating and evaluating accurate formal semantics and a corresponding analysis infrastructure, we leave generalizing the approach to other specification languages as future work.

### 8 RELATED WORK

**Modeling Kconfig specifications.** There are several prior efforts that convert Kconfig to logical formulas for various applications. Zengler et al. and Walch et al. modeled Kconfig in the DIMACS SAT format with the goal of finding Kconfig language metrics, including the number of options, types, and mandatory configuration options [37, 61]. She et al. describe a formal semantics [43] and a tool called LVAT that converts Kconfig specifications to the DIMACS SAT solver format [10, 44, 45]. It was designed for collecting statistics about the Kconfig language such as the number of options, the hierarchy of dependencies, and other metrics [10], rather than for precise formal verification of configuration specifications. Tool development appears to have stopped for LVAT in 2013 [42]. The undertaker project has a tool to convert Kconfig’s dumpconf output into the DIMACS SAT format for use in identifying code blocks in unpreprocessed C code [4, 53]. The kconfigreader tool converts the output of a Kconfig call dumpconf, which dumps each configuration options’ constraint expressions, into the DIMACS SAT solver format [25, 30]. El-Sharkawy et al., describes an informal semantics of Kconfig, provides illustrative examples, and evaluates the limitations of other tools [15]. Fernandez et al. described informal semantics for Kconfig constructs that they identified as incorrectly supported in prior conversion tools [16]. They provide a set of example Kconfig constructs that illustrate these limitations, which we have incorporated into kclause’s test suite. Fernandez et al. also describe a new conversion tool that produces Binary Decision Diagrams but has not been evaluated on Linux Kconfig specifications.

**Analyses of other configuration languages.** Shambaugh et al. [41] perform formal verification of the Puppet deployment configuration language to detect non-deterministic system state updates and other undesirable system configurations. Weiss et al. [59] automate Puppet configuration repair using formal reasoning over a propositional model of the language. Anderson et al. [8] formally verify the SmartFrog infrastructure deployment language to prove properties such as termination of compilation, comparing multiple implementations of SmartFrog compilers. Sotiropoulos et al. formally modeled the system call trace of the Puppet tool to find faults from ordering violations on resource usage [49]. Horton and Parlin infer system dependencies from Python code in order to generate Docker specification files [22]. They also inferred dependencies from Python code snippets to check if their package dependencies are out of date [23]. Bouchet et al. use formal verification to check for inadvertent public access to Amazon S3 instances [12]. Chenygyuan et al. mined frequently used dependencies between entities from deployment descriptors for Java-EE-platform-based applications to validate if a new deployment descriptor is violating mined dependencies [60]. Hanappi et al. formally modeled configuration scripts and resource usage to test if a system can recover from failures such as network outages and reach a stable state [21].

**Studies on variability bugs.** Some prior work extracted variability information from Makefiles and source code for finding bugs, dead code blocks, or inconsistencies between variability specification and implementation. [11, 14, 19, 36, 37, 48, 52]. Prior work also analyzed bugs or warnings raised from sampled configurations to classify them and understand how they are introduced [33, 34]. Similar analyses were performed on the bugs or vulnerabilities reported in the bug database or source commits [6, 7, 17, 35]. Others studied configuration sampling algorithms to find more variability bugs with fewer samples [29, 32, 46, 55].

### 9 CONCLUSION

We have introduced a new formal semantics and model checking infrastructure for analyzing Kconfig specification files and methodically derived a bug-finder, called kismet, for unmet dependencies, a common pitfall for Kconfig maintainers. Our results show that our bug-finder is precise, fast, and has resulted in patches to the mainline Linux kernel source code confirmed and accepted by maintainers. Future work includes continuing to repair all bugs found by kismet, applying it to ongoing kernel development and other software, and applying our analysis framework to other maintenance challenges.

We also plan to explore applying these model checking principles to other configuration specification languages to further improve the state of language tooling for software operations at large. As software operations are further automated, the languages used for configuring, building, and deploying software become an increasingly large component of the source code. These languages introduce new opportunities for less traditional software vulnerabilities, such as security misconfiguration. As our work demonstrates, these languages lend themselves to automated analysis, suggesting the future benefits of applying rigorous design and automated reasoning to software operations languages in general.

### ACKNOWLEDGMENTS

We would like to thank the anonymous referees for their valuable comments and helpful suggestions, Julia Lawall for advice and input into the work, and Elaine Weyuker for her feedback. This work is supported by the National Science Foundation under CCF-1941816 and CCF-1840934.
Finding Broken Linux Configuration Specifications by Statically Analyzing the Kconfig Language

ESEC/FSE ’21, August 23–28, 2021, Athens, Greece


