Understanding Memory and Thread Safety Practices and Issues in Real-World Rust Programs

Anonymous Author(s)

Abstract

Rust is a young programming language designed for systems software development. It aims to provide safety guarantees like high-level languages *and* performance efficiency like low-level languages. The core design of Rust is a set of strict safety rules enforced by compile-time checking. To support more low-level controls, Rust allows programmers to bypass these compiler checks to write *unsafe* code.

It is important to understand what safety issues exist in real Rust programs and how Rust safety mechanisms impact programming practices. We performed the first empirical study of Rust by close, manual inspection of 850 unsafe code usages and 170 bugs in five open-source Rust projects, five widely-used Rust libraries, two online security databases, and the Rust standard library. Our study answers three important questions: how and why do programmers write unsafe code, what memory-safety issues real Rust programs have, and what concurrency bugs Rust programmers make. Our study reveals interesting real-world Rust program behaviors and new issues Rust programmers make. Based on our study results, we propose several directions of building Rust bug detectors and built two static bug detectors, both of which revealed previously unknown bugs.

1 Introduction

Rust [71] is a programming language designed to build efficient *and* safe low-level software [8, 60, 64, 65]. Its main idea is to inherit most features in C and C's good runtime performance but to rule out C's safety issues with strict compile-time checking. Over the past few years, Rust has gained increasing popularity [40–42], especially in building low-level software like OSes and browsers [47, 51, 59, 62, 68].

The core of Rust's safety mechanisms is the concept of *ownership*. The most basic ownership rule allows each value to have only one *owner* and the value is freed when its owner's *lifetime* ends. Rust extends this basic rule with a set of rules that still guarantee memory and thread safety. For example, the ownership can be *borrowed* or *transferred*, and multiple *aliases* can read a value. These safety rules essentially prohibit the combination of *aliasing* and *mutability*, and they are checked by Rust at compile time, leaving runtime performance as efficient as unsafe languages like C.

The above safety rules Rust enforces limit programmers' control over low-level resources and are often overkill when delivering safety. To provide more flexibility to system programmers, Rust adds the support of *unsafe* code, code that bypasses main compiler safety checks. A function can be defined as unsafe or a piece of code inside a function can be unsafe. For the latter, the function can be called as a safe function in safe code, a pattern we call *interior unsafe*.

Although Rust's core safety design is simple and sound, it does not and is not intended to prevent all types of bugs. Moreover, programming rules in Rust are complex and very different from traditional languages, and Rust's strict compile-time checks further limit programming flexibility. Several recent works [2, 13, 24, 25] formalize and theoretically prove (a subset of) Rust's safety and interior-unsafe mechanisms. However, it is unclear how Rust's language designs affect real-world Rust developers, whether or not real Rust software still have issues, and if so what those issues are. With the wider adoption of Rust in systems software in recent years, it is important to answer these questions and understand real-world Rust program behaviors.

In this paper, we conduct the first empirical study on safety practices and safety issues in real-world Rust programs. We broadly define "safety" to be program safety and correctness, including both memory safety (*i.e.* no illegal memory accesses) and thread safety (*i.e.* threads can proceed without unintentional blocking and accesses to shared data are correct). Our study has a particular focus on how Rust's ownership and lifetime rules impact developers' programming and how the misuse of these rules causes safety issues, since these are Rust's unique and key features.

Our study covers five Rust-based systems and applications (two OSes, a browser, a key-value store system, and a blockchain system), five widely-used Rust libraries, and two online vulnerability databases. We analyzed their source code, their GitHub commit logs and issues, and publicly reported bugs by first filtering them into a small relevant set and then manually inspecting this set. In total, we studied 850 unsafe code usages, 70 memory-safety issues, and 100 thread-safety issues.

Our study includes three parts. First, we study how unsafe code is used, changed, and encapsulated. We found that unsafe code is extensively used in all of our studied Rust software and it is usually used for good reasons (*e.g.*, performance, code reuse), although programmers also try to reduce unsafe usages when they can. We further found that programmers use interior unsafe as a good practice to encapsulate unsafe code. However, explicitly and properly checking interior unsafe code can be difficult. Sometimes safe encapsulation is achieved by providing correct inputs and environments.

Second, we study memory-safety issues in real Rust programs by inspecting bugs in our selected applications and libraries and by examining *all* Rust issues reported on CVE [12] and RustSec [57]. We not only analyze these bugs' behaviors but also understand how the root causes of them are propagated to the effect of them. We found that all memory-safety bugs involve unsafe code, and (surprisingly) most of them also involve safe code. Mistakes are easy to happen when programmers write safe code without the caution of other related code being unsafe. We also found that the scope of *lifetime* in Rust is difficult to reason about, especially when combined with unsafe code, and wrong understanding of *lifetime* causes many memory-safety issues.

Finally, we study concurrency bugs, including non-blocking and blocking bugs [70]. Surprisingly, we found that non-blocking bugs can happen in both unsafe and safe code and that *all* blocking bugs we studied are in safe code. Although many bug patterns in Rust follow traditional concurrency bug patterns (*e.g.*, double lock, atomicity violation), a lot of the concurrency bugs in Rust are caused by programmers' misunderstanding of Rust's (complex) lifetime and safety rules.

For all the above three aspects, we make insightful suggestions to future Rust programmers and language designers. For example, based on the understanding of real-world Rust usage patterns, we make recommendations on good programming practices; based on our summary of common buggy code patterns and pitfalls, we make concrete suggestions on the design of future Rust bug detectors and programming tools.

With our empirical study results, we conducted an initial exploration on detecting Rust bugs by building two static bug detectors (one for use-after-free bugs and one for double-lock bugs). In total, these detectors found ten previously unknown bugs in our studied Rust applications. These encouraging (initial) results demonstrate the value of our empirical study.

We believe that programmers, researchers, and language designers can use our study results and the concrete, actionable suggestions we made to improve Rust software development (better programming practices, better bug detection tools, and better language designs). Overall, this paper makes the following contributions.

- The first empirical study on real-world Rust program behaviors.
- Analysis of real-world usages of safe, unsafe, and interior-unsafe code, with close inspection of 850 unsafe usages and 130 unsafe removals.
- Close inspection of 70 real Rust memory-safety issues and 100 concurrency bugs.
- 11 insights and 8 suggestions that can help Rust programmers and the future development of Rust.
- Two new Rust bug detectors and recommendations on how to build more Rust bug detectors.

A full report of all study results together with our bug detectors will be made public soon.

2 Background and Related Work

This section gives some background of Rust, including its history, safety (and unsafe) mechanisms, and its current support of bug detection, and overviews research projects on Rust related to ours.

2.1 Language Overview and History

Rust is a type-safe language designed to be both efficient and safe. It was designed for low-level software development where programmers desire low-level control of resources (so that programs run efficiently) but want to be type-safe and memory-safe. Rust defines a set of strict safety rules and uses the compiler to check these rules to statically rule out many potential safety issues. At runtime, Rust behaves like C and could achieve performance that is close to C.

Rust is the most loved language in 2019 according to a Stack Overflow survey [43], and it was ranked as the fifth fastest growing language on GitHub in 2018 [39]. Because of its safety and performance benefits, Rust's adoption in systems software has increased rapidly in recent years [3, 16, 22, 51, 59, 67, 68]. For example, Microsoft is actively exploring Rust as an alternative to C/C++ because of its memory-safety features [9, 38].

Rust was first released in 2012 and is now at version 1.39.0. Figure 1 shows the number of feature changes and LOC over the history of Rust. Rust went through heavy changes in the first four years since its release, and it has been stable since Jan 2016 (v1.6.0). With it being stable for more than three and a half years, we believe that Rust is now mature enough for an empirical study like ours. Figure 2 shows the fixed date of our analyzed bugs. Among the 170 bugs, 145 of them were fixed after 2016. Therefore, we believe our study results reflect the safety issues under stable Rust versions.

2.2 Safety Mechanisms

Rust's *safety* mechanism centers around the notion of *ownership*. At its core, Rust enforces a strict and restrictive rule of ownership: each value has one and only one *owner* variable, and when the owner's *lifetime* ends, the value will be *dropped* (freed). The lifetime of a variable is the scope where it is valid (e.g., from its creation to the end of the function it is in or to the end of matching parentheses), and it is detected and enforced by the Rust compiler.

Under Rust's basic ownership rule, a value has one exclusive owner. Rust extends this basic rule with a set of features to support more programming flexibility while still ensuring memory- and thread-safety. These features (as explained below) relax the restriction of having only one owner for the lifetime of a value but still *prohibit having aliasing and mutation at the same time*, and Rust statically checks these extended rules at compile time.

Ownership move. The ownership of a value can be *moved* from one *scope* to another, for example, from a caller to a callee and from one thread to another thread. The Rust

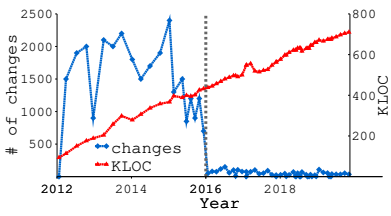

Figure 1. Rust History. *Each blue point shows the number of feature changes in one release version. Each red point shows total LOC in one release version.*

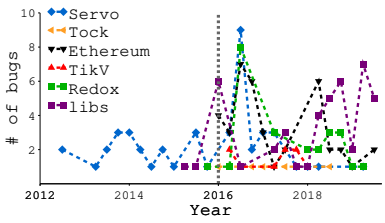

Figure 2. Time of Studied Bugs. *Each point shows the number of our studied bugs that were patched during a three month period.*

Software	Start Time	Stars	Commits	LOC	Mem	Blk	NBlk
Servo	2012/02	14574	38096	271K	14	13	18
Tock	2015/05	1343	4621	60K	5	0	2
Ethereum	2015/11	5565	12121	145K	2	33	4
TiKV	2016/07	5717	3897	149K	1	5	3
Redox	2016/08	11450	2129	199K	20	2	3
libraries	2010/07	3106	2402	25K	7	6	10

Table 1. Studied Applications and Libraries. *The start time, number of stars, and commits on GitHub, total source lines of code, the number of memory safety bugs, blocking bugs, and non-blocking bugs. libraries: maximum values among our studied libraries. There are 22 bugs collected from the two CVE databases.*

compiler statically guarantees that an owner variable cannot be accessed after its ownership is moved. As a result, a caller cannot access a value anymore if the value is dropped in the callee function, and a shared value can only be owned by one thread at any time.

Ownership borrowing. A value's ownership can also be *borrowed* temporarily to another variable for the lifetime of this variable without moving the ownership. Borrowing is achieved by passing the value by reference to the borrower variable. Rust does not allow borrowing ownership across threads, since a value's lifetime cannot be statically inferred across threads and there is no way the Rust compiler can guarantee that all usages of a value are covered by its lifetime.

Mutable and Shared references. Another extension Rust adds on top of the basic ownership rules is the support of multiple shared read-only references, *i.e.*, allowing read-only aliasing. A value's reference can also be *mutable*, allowing write access to the value, but there can only be one mutable reference at any single time. After borrowing a value's ownership through *mutable reference*, the temporary owner has the exclusive write access to the value.

2.3 Unsafe and Interior Unsafe

Rust's safety rules are strict and its static compiler checking for the rules is *conservative*. Developers (especially low-level software developers) often have the need to manage safety by themselves. Rust allows programs to bypass its safety checking with the *unsafe* feature, denoted by the keyword `unsafe`. A function can be marked as `unsafe`; a piece of code can be marked as `unsafe`; and a *trait* can be marked as `unsafe` (Rust traits are similar to interfaces in traditional languages like Java). Code regions marked with `unsafe` will bypass Rust's compiler checks and be able to perform four types of unsafe functionalities: dereferencing and manipulation of raw pointers, access and modification of mutable static variables (*i.e.*, global variables), calling unsafe functions, and implementing unsafe traits.

Rust allows a function to have unsafe code only internally; such a function can be called by safe code and thus is considered "safe" externally. We call this pattern *interior unsafe*.

The design rationale of interior unsafe code is to have the flexibility and low-level management of unsafe code but to encapsulate the unsafe code in a carefully-controlled interface, or at least that is the intention of the interior unsafe design. For example, Rust uses interior-unsafe functions to allow the combination of aliasing and mutation (*i.e.*, bypassing Rust's core safety rules) in a controlled way: the internal unsafe code can mutate values using multiple aliases, but these mutations are encapsulated in a small number of immutable APIs that can be called in safe code and pass Rust's safety checks. Rust calls this feature *interior mutability*.

Many APIs provided by the Rust standard library are interior-unsafe functions, such as `Arc`, `Rc`, `Cell`, `RefCell`, `Mutex`, and `RwLock`. Section 4.3 presents our analysis of interior unsafe usages in Rust standard library.

2.4 Bug Detection in Rust

Rust runtime detects and triggers a panic on certain types of bugs, such as buffer overflow, divided by zero and stack overflow. Rust also provides more bug-detecting features in its debug build mode, including detection of double lock and integer overflow. These dynamic detection mechanisms Rust provides only capture a small number of issues.

Rust uses LLVM [26] as its backend. Many static and dynamic bug detection techniques [4, 34, 78, 79] designed for C/C++ can also be applied to Rust. However, it is still valuable to build Rust-specific detectors, because Rust's new language features and libraries can cause new types of bugs as evidenced by our study.

The Rust team has released two memory-bug detectors. Rust-clippy [55] is a static detector for memory bugs that follow certain simple patterns (nine lints). It only covers a small amount of buggy patterns. Miri [37] is a dynamic memory-bug detector that interprets and executes Rust's mid-level intermediate representation (*MIR*). Its bug detection relies on users providing the inputs that can trigger memory bugs. It also generates many false positives. For example, Miri reports the creation of an uninitialized heap memory as a memory bug, failing to consider the false-positive case where the program writes to the memory first before performing any read.

In short, these existing Rust bug detection tools have their own limitations, and neither targets concurrency bugs.

An empirical study on Rust bugs like this work is important. It can help future researchers and practitioners to build Rust-specific detectors. In fact, we have built two detectors based on our findings in this study, both of which reveal previously undiscovered bugs.

2.5 Formalizing and Proving Rust's Correctness

Several previous works aim to formalize or prove the correctness of Rust programs [2, 13, 24, 25, 52]. RustBelt [24] conducts the first safety proof for a subset of Rust. Patina [52] proves the safety of Rust's memory management. Baranowski *et al.* extend the SMACK verifier to work on Rust programs [2]. After formalizing Rust's type system in CLP, Rust programs can be generated by solving a constraint satisfaction problem, and the generated programs can then be used to detect bugs in the Rust compiler [13]. K-Rust [25] compares the execution of a Rust program in K-Framework environment with the execution on a real machine to identify inconsistency between Rust's specification and the Rust compiler's implementation. Different from these works, our study aims to understand common mistakes made by real Rust developers, and it can improve the safety of Rust programs from a practical perspective.

2.6 Empirical Studies

In the past, researchers have conducted various empirical studies on different kinds of bugs in different programming languages [7, 19, 20, 23, 28, 32, 33]. As far as we know, we are the first study on real-world mistakes of Rust code.

There are only few empirical studies on Rust unsafe code usage similar to what we performed in Section 4. However, the scales of these studies are small on both the applications studied and the features studied. One previous study counts the number of Rust libraries that depend on external C/C++ libraries [63]. One study counts the amount of unsafe code in *crates.io* [44]. Another analyzes several cases where interior unsafe is not well encapsulated [45]. Our work is the first large-scale, systematic empirical study on unsafe in Rust. We study many aspects not covered by previous works.

3 Application and Methodology

Although there are many books, blogs, and theoretical publications that discuss Rust's design philosophy, benefits, and unique features, it is unclear how real-world Rust programmers use Rust and what pitfalls they make. We perform an empirical study on real-world Rust software. Before presenting our study results, this section first outlines our studied applications and our study methodology.

Studied Rust software and libraries. We selected five software systems written in Rust for our study (Table 1). They cover a wide range of software types, have relatively long history, and are popular and actively maintained.

Servo [59] is a browser engine developed by Mozilla. Servo has been developed side by side with Rust and has the longest history among the applications we studied. *TiKV* [67] is a key-value store that supports both single key-value-pair and transactional key-value accesses. *Parity Ethereum*[1] [46] is a fast, secure Ethereum client written in Rust (Ethereum [15] is an open software platform based on blockchain technology). *Redox* [51] is an open-source secure OS that adopts microkernel architecture but exposes UNIX-like interface. *Tock* [29] is a Rust-based embedded OS. Tock leverages Rust's compile-time memory-safety checking to isolate its OS modules.

Apart from the above five applications, we study five widely-used Rust libraries (also written in Rust). They include 1) *Rand* [48], a library for random number generation, 2) *Crossbeam* [10], a framework for building lock-free concurrent data structures, 3) *Threadpool* [66], Rust's implementation of thread pool, 4) *Rayon* [50], a library for parallel computing, and 5) *Lazy_static* [27], a library for defining lazily evaluated static variables.

Collecting and studying bugs. To collect bugs, we analyzed GitHub commit logs from applications in Table 1. We first filtered the commit logs using a set of safety-related keywords, *e.g.*, "use-after-free" for memory bugs, "deadlock" for concurrency bugs. These keywords either cover important issues in the research community [11, 72, 73] or are used in previous works to collect bugs [28, 30, 33, 70]. We then manually inspected filtered logs to identify bugs. For our memory-safety study, we also analyzed all Rust-related vulnerabilities in two online vulnerability databases, CVE [12] and RustSec [57]. In total, we studied 70 memory and 100 concurrency bugs.

We manually inspected and analyzed all available sources for each bug, including its patch, bug report, and online discussions. Each bug is examined by at least two people in our team. We also reproduced a set of bugs to validate our understanding. During our bug study, we identified common mistakes made by different developers in different projects. We believe similar mistakes can be made by other developers in many other Rust projects.

4 Unsafe Usages

There is a fair amount of unsafe code in Rust programs. We found 12835 unsafe usages in our studied applications in Table 1, including 7061 unsafe code regions, 5727 unsafe functions, and 47 unsafe traits. In Rust's standard library (Rust std for short), we found 1577 unsafe code regions, 870 unsafe functions, and 12 unsafe traits.

Since `unsafe` code bypasses compiler safety checks, understanding unsafe usages is an important aspect of studying safety practice in reality. We randomly select 600 unsafe usages from our studied applications, including 400 interior

[1] In this paper, we call Parity Ethereum by Ethereum for brevity.

unsafe usages and 200 unsafe functions. We also studied 250 interior unsafe usages in Rust std. We manually inspect these unsafe usages to understand 1) why unsafe is used in the latest program versions, 2) how unsafe is removed during software evolution, and 3) how interior unsafe is encapsulated.

4.1 Reasons of Usage

To understand how and why programmers write unsafe code, we first inspect the type of operations these unsafe usages are performing. Most of them (66%) are for (unsafe) memory operations, such as raw pointer manipulation and type casting. Calling unsafe functions counts for 29% of the total unsafe usages. Most of these calls are made to unsafe functions programmers write themselves and functions written in other languages. In Rust std, heaviest unsafe usages appear in the *sys*, *thread* and *sync* modules, likely because they interact more with low-level systems.

To understand the reasons why programmers use unsafe code, we further analyze the *purposes* of our studied 600 unsafe usages. The most common purpose of the unsafe usages is to reuse existing code (42%), for example, to convert a C-style array to Rust's variable-size array (called *slice*), to call functions from external libraries like *glibc*. Another common purpose of using unsafe code is to improve performance (22%). We wrote simple tests to evaluate the performance difference between some of the unsafe and safe code that can deliver the same functionalities. Our experiments show that unsafe memory copy with `ptr::copy_nonoverlapping()` is 23% faster than the `slice::copy_from_slice()` in some case. Unsafe memory access with `slice::get_unchecked()` is 4-5× faster than the safe memory access with boundary checking. Traversing an array by pointer computing (`ptr::offset()`) and dereferencing is also 4-5× faster than the safe array access with boundary checking. The remaining unsafe usages include bypassing Rust's safety rules to share data across threads (14%) and other types of Rust compiler check bypassing.

One interesting finding is that programmers sometimes mark a function as unsafe just as a warning of possible dangers in using this function, and removing these `unsafe` will not cause any compile errors (32 or 5% of the unsafe usages we studied).

Five unsafe usages in our studied applications and 56 in Rust std are for labeling struct constructors. These constructors only contain safe operations (*e.g.*, initializing struct fields using input parameters), but other functions in the struct can perform unsafe operations and their safety depends on safe initialization of the struct. For example, in Rust std, the `slice` struct has a constructor function `slice::from_raw_parts()` which creates a `slice` using the input of a pointer and a length (together representing a memory space). `slice::from_raw_parts()` is marked as an unsafe function although the operations in it are all safe. Other functions in `slice` that use the memory space are the ones that could potentially have safety issues. Instead of marking all these functions unsafe and requiring programmers to properly check safe conditions when using them, it is more efficient and reliable to mark only the constructor as unsafe, essentially *encapsulating* the unsafe nature in a much smaller scope. Similar usages also happen in applications, and explained by developers as good practice [69].

Insight 1: *Most unsafe usages are for good or unavoidable reasons, indicating that Rust's rule checks are sometimes too strict and that it is useful to provide an alternative way to escape these checks.*

Suggestion 1: *Programmers should try to find the source of unsafety and only export that piece of code as an* `unsafe` *interface to minimize* `unsafe` *interfaces and to reduce code inspection efforts.*

4.2 Unsafe Removal

Although most of the unsafe usages we found are for good reasons, programmers sometimes remove unsafe code or change them to safe ones. We analyzed 108 randomly selected commit logs that contain cases where `unsafe` is removed (130 cases in total). The purposes of these unsafe code removals include improving memory safety (72%), better code structure (19%), improving thread safety (3%), bug fixing (3%), and removing unnecessary usages (2%).

Among our analyzed commit logs, 55 cases completely change unsafe code to safe code. The remaining cases change unsafe code to interior unsafe code, with 33 interior unsafe functions in Rust std, 28 self-implemented interior unsafe functions, and 14 third-parity interior unsafe functions. By encapsulating unsafe code in an interior unsafe function that can be safely called at many places, programmers only need to ensure the safety in this one interior unsafe function (*e.g.*, by checking conditions) instead of performing similar checks at every usage of the unsafe code.

Insight 2: *Interior unsafe is a good way to encapsulate unsafe code.*

Suggestion 2: *Rust developers should first try to properly encapsulate unsafe code in interior unsafe functions before exposing them as unsafe.*

4.3 Encapsulating Interior Unsafe

With unsafe code being an essential part of Rust software, it is important to know what are the good practices when writing unsafe code. From our analysis results above and from Rustonomicon [56], encapsulating unsafe code with interior unsafe functions is a good practice. But it is important to understand how to properly write such encapsulation.

To answer this question, we first analyze how Rust std encapsulates interior unsafe code (by both understanding the code and reading its comments and documentation). Rust std

```
1 impl<T, ...> Queue<T, ...> {
2     pub fn pop(&self) -> Option<T> { unsafe {...}}
3     pub fn peek(&self) -> Option<&mut T> { unsafe {...}}
4 }
5 // let e = Q.peek().unwrap();
6 // {Q.pop()}
7 // println!("{}", *e); < - use after free
```

Figure 3. An interior mutability example from Rust std.

interior unsafe functions are called heavily by Rust software. It is important to both learn from how std encapsulates unsafe code and examine if there is any issue in such encapsulation.

In total, we sampled 250 interior unsafe functions in Rust std. For the unsafe code to work properly, different types of conditions need to be satisfied. For example, 68% of interior unsafe code regions require valid memory space or valid UTF-8 characters. 15% require conditions in lifetime or ownership.

We then examined how Rust std ensures that these conditions are met. Surprisingly, Rust std does not perform any explicit condition checking in most of its interior unsafe functions (58%). Instead, it ensures that the input or the environment that the interior unsafe code executes with is safe. For example, the unsafe function `Arc::from_raw()` always takes input from the return of `Arc::into_raw()` in all sampled interior unsafe functions. Rust std performs explicit checking for the rest of the interior unsafe functions, *e.g.*, by confirming that an index is within the memory boundary.

After understanding std interior unsafe functions, we inspect 400 sampled interior unsafe functions in our studied applications. We have similar findings from these application-written interior unsafe functions.

Worth noticing is that we identified 19 cases where interior unsafe code is improperly encapsulated, including five from the std and 14 from the applications. Although they have not caused any real bugs in the applications we studied, they may potentially cause safety issues if they are not used properly. Four of them do not perform any checking of return values from external library function calls. Four directly dereference input parameters or use them directly as indices to access memory without any boundary checking. Other cases include not checking the validity of function pointers, using type casting to change objects' lifetime to static, and potentially accessing uninitialized memory.

Of particular interest are two bad practices that lead to potential problems. They are illustrated in Figure 3. Function `peek()` returns a reference of the object at the head of a queue, and `pop()` pops (removes) the head object from the queue. A use-after-free error may happen with the following sequence of operations (all safe code): a program first calls `peek()` and saves the returned reference at line 5, then calls `pop()` and drop the returned object at line 6, and finally uses the previously saved reference to access the (dropped) object at line 7. This potential error is caused by holding an immutable reference while changing the underlying object. This operation is allowed by Rust because both functions take an immutable reference `&self` as input. When these functions are called, the ownership of the queue is immutably borrowed to both functions.

According to the program semantics, `pop()` actually changes the immutably borrowed queue. This *interior mutability* (see Section 2.3 for definition) is improperly written, which results in the potential error. An easy way to avoid this problem is to change the input parameter of `pop()` to `&mut self`. When a queue is immutably borrowed by `peek()` at line 5, the borrowing does not end until line 7, since the default lifetime rule extends the lifetime of `&self` to the lifetime of the returned reference [54]. After the change, the Rust compiler will not allow the mutable borrow by `pop()` at line 6.

Insight 3: *Some safety conditions of unsafe code are difficult to check. Interior unsafe functions often rely on the preparation of correct inputs and/or execution environments for their internal unsafe code to be safe.*

Suggestion 3: *If a function's safety depends on how it is used, then it is better marked as unsafe not interior unsafe.*

Suggestion 4: *Interior mutability can potentially violate Rust's ownership borrowing safety rules, and Rust developers should restrict its usages and check all possible safety violations, especially when an interior mutability function returns a reference. We also suggest Rust designers differentiate interior mutability from real immutable functions.*

5 Memory Safety Issues

Memory safety is a key design goal of Rust. Rust uses a combination of static compiler checks and dynamic runtime checks to ensure memory safety for its safe code. However, it is not clear whether or not there are still memory-safety issues in real Rust programs, especially when they commonly include unsafe and interior-unsafe code. This section presents our detailed analysis of 70 real-world Rust memory-safety issues and their fixes.

5.1 Bug Analysis Results

It is important to understand both the *cause* and the *effect* of memory-safety issues (bugs). We categorize our studied bugs along two dimensions: how errors propagate and what are the effects of the bugs. Table 2 summarizes the results in the two dimensions introduced above.

For the first dimension, we analyze the error propagation chain from a bug's cause to its effect and consider how safety semantics change during the propagation chain. Similar to prior bug analysis methodologies [78, 79], we consider the code where a bug's patch is applied as its cause and the code where the error symptom can be observed as its effect. Based on whether cause and effect are in safe or unsafe code, we categorize bugs into four groups: safe → safe (or simply, safe), safe → unsafe, unsafe → safe, and unsafe → unsafe (or simply, unsafe).

Category	Wrong Access			Lifetime Violation			Total
	Buffer	Null	Uninitialized	Invalid	UAF	Double free	
safe	0	0	0	0	1	0	1
unsafe ⋆	3 (1)	12 (5)	0	5 (3)	0	0	20 (9)
safe → unsafe ⋆	18 (10)	0	0	1	11 (3)	2 (2)	32 (15)
unsafe → safe	0	0	7	4	2	4	17

Table 2. Memory Bugs Category. *Buffer: Buffer overflow; Null: Null pointer dereferencing; Uninitialized: Read uninitialized memory; Invalid: Invalid free; UAF: Use after free. ⋆: numbers in () are for bugs whose effects are in interior-unsafe functions.*

```
1 pub struct FILE {
2     buf: Vec<u8>,
3 }
4
5 pub unsafe fn _fdopen(...) {
6     let f = alloc(size_of::<FILE>()) as * mut FILE;
7 -   *f = FILE{buf: vec![0u8; 100]};
8 +   ptr::write(f, FILE{buf: vec![0u8; 100]});
9 }
```

Figure 4. An invalid-free bug in Redox.

For the second dimension, we categorize bug effects into wrong memory accesses (*e.g.*, buffer overflow) and lifetime violations (*e.g.*, use after free).

Buffer overflow. 18 out of 21 bugs in this category follow the same pattern: an error happens when computing buffer size or index in safe code and an out-of-boundary memory access happens later in unsafe code. For 11 bugs, the effect is inside an interior unsafe function. Six interior unsafe functions contain condition checks to avoid buffer overflow. However, the checks do not work due to wrong checking logic, inconsistent struct status, or integer overflow. For three interior functions, their input parameters are used directly or indirectly as an index to access a buffer, without any boundary checks.

Null pointer dereferencing. All bugs in this category are caused by dereferencing a null pointer in unsafe code. In five of them, null pointer dereferencing happens in an interior unsafe function. These interior unsafe functions do not perform proper checking as the good practices in Section 4.3.

Reading uninitialized memory. All the seven bugs in this category are unsafe → safe. Four of them use unsafe code to create an uninitialized buffer and later read it using safe code. The rest initialize buffers incorrectly, *e.g.*, using memcpy with wrong input parameters.

Invalid free. Out of the ten invalid-free bugs, five share the same (unsafe) code pattern. Figure 4 shows one such example. The variable `f` is a pointer pointing to an uninitialized memory buffer with the same size as struct `FILE` (line 6). Assigning a new `FILE` struct to `*f` at line 7 ends the lifetime of the previous struct `f` points to, causing the previous struct to be dropped by Rust. All the allocated memory with the previous struct will be freed, (*e.g.*, memory in `buf` at line 2). However, since the previous struct contains uninitialized memory buffer, freeing its heap memory is invalid. Note that such behavior is unique to Rust and does not happen in traditional languages (*e.g.*, `*f=buf` in C/C++ does not cause the object pointed by `f` to be freed).

```
1  pub fn sign(data: Option<&[u8]>) {
2 -  let p = match data {
3 -    Some(data) => BioSlice::new(data).as_ptr(),
4 -    None => ptr::null_mut(),
5 -  };
6 +  let bio = match data {
7 +    Some(data) => Some(BioSlice::new(data)),
8 +    None => None,
9 +  };
10 +  let p = bio.map_or(ptr::null_mut(),|p| p.as_ptr());
11    unsafe {
12      let cms = cvt_p(CMS_sign(p));
13    }
14  }
```

Figure 5. A use-after-free bug in RustSec.

Use after free. 11 out of 14 use-after-free bugs happen because an object is dropped implicitly in safe code (when its lifetime ends), but a pointer to the object or to a field of the object still exists and is later dereferenced in unsafe code. Figure 5 shows an example. When the input `data` is valid, a `BioSlice` object is created at line 3 and its address is assigned to a pointer `p` at line 2. `p` is used to call an unsafe function `CMS_sign()` at line 12 and it is dereferenced inside that function. However, the lifetime of the `BioSlice` object ends at line 5 and the object will be dropped there. The use of `p` is thus after the object has been freed. Both this bug and the bug in Figure 4 are caused by wrong understanding of object lifetime. We have identified misunderstanding of lifetime being the main reason for most use-after-free and many other types of memory-safety bugs.

There is one use-after-free bug whose cause and effect are both in safe code. This bug occurred with an early Rust version (v0.3) and the buggy code pattern is not allowed by the Rust compiler now. The last two bugs happen in a self-implemented vector. Developers explicitly drop the underlying memory space in unsafe code due to some error in condition checking. Later accesses to the vector in safe code trigger an use-after-free error.

Double free. There are six double-free bugs. Other than two bugs that are safe → unsafe and similar to traditional double-free bugs, the rest are all unsafe → safe and unique to Rust. These buggy programs first conduct some unsafe memory operation to create two owners of a value. When these owners' lifetime ends, their values will be dropped (twice), causing double free. One such bug is caused by

```
t2 = ptr::read::<T>(&t1)
```

which reads the content of `t1` and puts it into `t2` without moving `t1`. If type `T` contains a pointer field that points to some object, the object will have two owners, `t1` and `t2`. When `t1` and `t2` are dropped by Rust implicitly when their lifetime ends, double free of the object happens. A safer way is to move the ownership from `t1` to `t2` using `t2 = t1`. These ownership rules are unique to Rust and programmers need to be careful when writing similar code.

Insight 4: *Rust's safety mechanisms (in Rust's stable versions) are very effective in preventing memory bugs. All*

memory-safety issues involve unsafe code (although many of them also involve safe code).

Suggestion 5: *Future memory bug detectors can ignore safe code that is unrelated to unsafe code to reduce false positives and to improve execution efficiency.*

5.2 Fixing Strategies

We examine how our collected memory-safety bugs were fixed and categorize their fixing strategies into four categories.

Conditionally skip code. 30 bugs were fixed by capturing the conditions that lead to dangerous operations and skipping the dangerous operations under these conditions. For example, when the offset into a buffer is outside its boundary, buffer accesses are skipped. 25 of these bugs were fixed by skipping unsafe code, two were fixed by skipping interior unsafe code, and three skipped safe code.

Adjust lifetime. 23 bugs were fixed by changing the lifetime of an object to avoid it being dropped improperly. These include extending the object's lifetime to fix use-after-free (*e.g.*, the fix of Figure 5), changing the object's lifetime to be bounded to a single owner to fix double-free, and avoiding the lifetime termination of an object when it contains uninitialized memory to fix invalid free (*e.g.*, the fix of Figure 4).

Change unsafe operands. Nine bugs were fixed by modifying operands of unsafe operations, such as providing the right input when using `memcpy` to initialize a buffer and changing the length and capacity into a correct order when calling `Vec::from_raw_parts()`.

Other. The remaining eight bugs used various fixing strategies outside the above three categories. For example, one bug was fixed by correctly zero-filling a created buffer. Another bug was fixed by changing memory layout.

Insight 5: *More than half of memory-safety bugs were fixed by changing or conditionally skipping unsafe code, but only few were fixed by completely removing unsafe code, suggesting that unsafe code is unavoidable in many cases.*

6 Thread Safety Issues

Rust provides unique thread-safety mechanisms to help prevent concurrency bugs, and as Rust language designers put it, to achieve "fearless concurrency" [53]. However, we have found a fair amount of concurrency bugs. Similar to a recent work's taxonomy of concurrency bugs [70], we divide our 100 collected concurrency bugs into blocking bugs (*e.g.*, deadlock) and non-blocking bugs (*e.g.*, data race).

This section presents our analysis on the root causes and fixing strategies of our collected blocking and non-blocking bugs, with a particular emphasis on how Rust's ownership and lifetime mechanisms and its unsafe usages impact concurrent programming.

Software	Mutex&Rwlock	Condvar	Channel	Once	Other
Servo	6	0	5	0	2
Tock	0	0	0	0	0
Ethereum	26	6	0	0	1
TiKV	4	1	0	0	0
Redox	2	0	0	0	0
libraries	0	3	1	1	1
Total	38	10	6	1	4

Table 3. Types of Synchronization in Blocking Bugs.

6.1 Blocking Bugs

Blocking bugs manifest when one or more threads conduct operations that wait for resources (blocking operations), but these resources are never available. In total, we studied 59 blocking bugs. All of them are caused by using interior unsafe functions in safe code.

Bug Analysis. We study blocking bugs by examining what blocking operations programmers use in their buggy code and how the blocking conditions happen. Table 3 summarizes the number of blocking bugs that are caused by different blocking operations. 55 out of 59 blocking bugs are caused by operations of synchronization primitives, like `Mutex` and `Condvar`. All these synchronization operations have safe APIs, but their implementation heavily uses interior-unsafe code, since they are primarily implemented by reusing existing libraries like pthread. The other four bugs are not caused by primitives' operations (one blocked at an API call only on Windows platform, two blocked at a busy loop, and one blocked at `join()` of threads).

`Mutex` and `RwLock`. Different from traditional multi-threaded programming languages, the locking mechanism in Rust is designed to protect data accesses, instead of code fragments [36]. To allow multiple threads to have write accesses to a shared variable in a safe way, Rust developers can declare the variable with both `Arc` and `Mutex`. The `Lock()` function returns a reference of the shared variable and *locks* it. The Rust compiler verifies that all accesses to the shared variable are conducted with the lock being held, guaranteeing mutual exclusion. A lock is automatically released when the lifetime of the returned variable holding the reference ends (the Rust compiler implicitly calls `Unlock()` when the lifetime ends).

Failing to acquire `Lock` (for `Mutex`) or `read`/`write` (for `RwLock`) results in thread blocking for 38 bugs, with 30 of them caused by double locking, seven caused by acquiring locks in conflicting orders, and one caused by forgetting to unlock when using a self-implemented mutex. Even though problems like double locking and conflicting lock orders are common in traditional languages too, Rust's complex lifetime rules together with its implicit unlock mechanism make it harder for programmers to write blocking-bug-free code.

Figure 6 shows a double-lock bug. The variable `client` is an `Inner` object protected by an `RwLock`. At line 3, its `read` lock is acquired and its `m` field is used as input to call function `connect()`. If `connect()` returns `Ok`, the `write` lock is acquired at line 7 and the `inner` object is

```
1  fn do_request() {
2    //client: Arc<RwLock<Inner>>
3  - match connect(client.read().unwrap().m) {
4  + let result = connect(client.read().unwrap().m);
5  + match result {
6      Ok(_) => {
7        let mut inner = client.write().unwrap();
8        inner.m = mbrs;
9      }
10     Err(_) => {}
11   };
12 }
```

Figure 6. A double-lock bug in TiKV.

modified at line 8. The `write` lock at line 7 will cause a double lock, since the lifetime of the temporary reference-holding object returned by `client.read()` spans the whole `match` code block and the read lock is held until line 11. The patch is to save to the return of `connect()` to a local variable to release the read lock at line 4, instead of using the return directly as the condition of the `match` code block.

This bug demonstrates the unique difficulty in knowing the boundaries of critical sections in Rust. Rust developers need to have a good understanding of the lifetime of a variable returned by `Lock`, `read`, or `write` to know when `Unlock()` will implicitly be called. But Rust's complex language features make it tricky to determine lifetime scope. For example, in five double-lock bugs, the first lock is in a `match` condition and the second lock is in the corresponding `match` body (*e.g.*, Figure 6). In another five double-lock bugs, the first lock is in an `if` condition, and the second lock is in the `if` block or the `else` block. The unique nature of Rust's locking mechanism to protect data accesses makes the double-lock problem even more severe, since mutex-protected data can only be accessed after calling `Lock()`.

`Condvar`. In eight of the ten bugs related to `Condvar`, one thread is blocked at `wait()` of a `Condvar`, while no other threads invoke `notify_one()` or `notify_all()` of the same `Condvar`. In the other two bugs, one thread is waiting for a second thread to release a lock, while the second thread is waiting for the first to invoke `notify_all()`.

Channel. In Rust, a channel has unlimited buffer size by default, and pulling data from an empty channel blocks a thread until another thread sends data to the channel. There are five bugs caused by blocking at receiving operations. In one bug, one thread blocks at pulling data from a channel, while no other threads can send data to the channel. For another three bugs, two or more threads wait for data from a channel but fail to send data other threads wait for. In the last bug, one thread holds a lock while waiting for data from a channel, while another thread blocks at lock acquisition and cannot send its data.

Rust also supports synchronous channel with a bounded buffer size. When the buffer of a synchronous channel is full, sending data to the channel will block a thread. There is one bug that is caused by a thread being blocked when sending to a full channel.

`Once`. `Once` is designed to ensure that a global variable is only initialized once. The initialization code can be put into a closure and used as the input parameter of `call_once()` method of an `Once` object. Even when multiple threads call `call_once()` multiple times, only the first invocation is actually executed. However, when the input closure of `call_once()` recursively calls `call_once()` of the same `Once` object, a deadlock will be triggered. We have one bug of this type.

Insight 6: *The lack of a good understanding of Rust's lifetime rules is a common cause for many blocking bugs.*

Suggestion 6: *Future IDEs should add plug-ins to highlight the location of Rust's implicit unlock, which could help Rust developers avoid many blocking bugs.*

Fixing Blocking Bugs. Most of the Rust blocking bugs we collected (50/59) were fixed by adjusting synchronization operations, including adding new operations, removing unnecessary operations, and moving or changing existing operations. One fixing strategy unique to Rust is adjusting the lifetime of the returned variable of `Lock` (or `read`, `write`) to change the location of the implicit `Unlock()`. This strategy was used for the bug of Figure 6 and 16 other bugs. Adjusting the lifetime of a variable is much harder than moving an explicit `Unlock()` as in traditional languages.

The other nine blocking bugs were not fixed by adjusting synchronization mechanisms. For example, one bug was fixed by changing a blocking system call into a non-blocking one.

One strategy to avoid blocking bugs is to explicitly define the boundary of a critical section. Rust allows explicit drop of the return value of `Lock` (by calling `mem::drop()`). We found 11 such usages in our studied applications. Among them, nine cases perform explicit drop to avoid double lock and one case is to avoid acquiring locks in conflicting orders. Although effective, this method is not always convenient, since programmers may want to use `Lock` functions directly without saving their return values (*e.g.*, the `read` lock is used directly at line 3 in Figure 6).

Suggestion 7: *Rust should add an explicit unlock API of `Mutex`, since programmers may not save the return value of `Lock` in a variable and explicitly dropping the return value is sometimes inconvenient.*

6.2 Non-Blocking Bugs

Non-blocking bugs are concurrency bugs where all threads can finish their execution, but with undesired results. This part presents our study on non-blocking bugs.

Rust supports both shared memory and message passing as mechanisms to communicate across threads. Among the 41 non-blocking bugs, four are caused by errors in message passing (*e.g.*, messages in an unexpected order causing programs

Software	Unsafe/Interior-Unsafe				Safe		MSG
	Global	Pointer	Ref	O. H.	Atomic	Mutex	
Servo	1	7	1	0	0	6	3
Tock	0	0	0	2	0	0	0
Ethereum	0	0	0	0	1	2	1
TiKV	0	0	0	1	1	1	0
Redox	1	0	0	2	0	0	0
libraries	1	6	1	0	3	0	0
Total	3	13	2	5	5	9	4

Table 4. How threads communicate. *Global: global static mutable integer; Ref: RefCell; O. H.: OS or hardware resources.*

to misbehave). All the rest are caused by failing to protect shared resources. Since there are only four bugs related to message passing, we mainly focus our study on non-blocking bugs caused by shared memory, unless otherwise specified.

Data Sharing in Buggy Code. Errors during accessing shared data are the root causes for most non-blocking bugs in traditional programming languages [6, 14, 17, 34, 58, 76]. Rust's core safety rules forbid mutable aliasing, which essentially disables mutable sharing across threads. For non-blocking bugs like data races to happen, some data must have been shared and modified. It is important to understand how real buggy Rust programs share data across threads, since differentiating shared variables from local variables can help the development of various bug detection tools [21]. We analyzed how the 37 non-blocking bugs share data and categorized them in Table 4.

Sharing with unsafe code. 23 non-blocking bugs share data using unsafe code, out of which 20 use interior-unsafe functions to share data. Without a detailed understanding of the interior-unsafe functions and their internal unsafe mechanisms, developers may not even be aware of the shared-memory nature when they call these functions.

The most common way to share data is by passing a raw pointer to a memory space (13 in our non-blocking bugs). A thread can store the pointer in a local variable and later dereference it or cast it to a reference. All raw pointer operations are unsafe, although after (unsafe) casting, accesses to the casted reference can be in safe code. Many Rust applications are low-level software. We found the second most common type of data sharing (5) to be accessing OS system calls and hardware resources (through unsafe code). For example, in one bug, multiple threads share the return value of the system call `getmntent`, which is a pointer to a structure containing fields describing a file system. The other two unsafe data-sharing methods used in the remaining 5 bugs are accessing static mutable variables which is only allowed in unsafe code, and implementing unsafe `Sync` trait for a struct with `RefCell` as a field.

Sharing with safe code. A value can be shared across threads in safe code if the Rust compiler can statically determine that all threads' accesses to it are within its lifetime and that there can only be one writer at a time. Even though the sharing of any single value in safe code follows Rust's safety rules (*i.e.*, no combination of aliasing and mutability), bugs still happen because of violations to programs' semantics (often involving more than one value). 14 non-blocking bugs share data with safe code, and we categorize them in two dimensions. To guarantee mutual exclusion, five of them use atomic variables as shared variables, and the other nine bugs wrap shared data using `Mutex` (or `RwLock`). To ensure lifetime covers all usages, eight bugs use `Arc` to wrap shared data and the other six bugs use global variables as shared variables.

Insight 7: *There are patterns of how data is (improperly) shared and these patterns are useful when designing bug detection tools.*

Bug Analysis. After a good understanding of how Rust programmers share data across threads, we further examine the non-blocking bugs to see how programmers make mistakes. Although there are many unique ways Rust programmers share data, they still make traditional mistakes that cause non-blocking bugs. These include data race [14, 58, 76], atomicity violation [6, 17, 34], and order violation [18, 35, 75, 79].

We examine how shared memory is synchronized for all our studied non-blocking bugs. 15 of them do not synchronize (protect) the shared memory accesses at all, and the memory is shared using unsafe code. This result shows that using unsafe code to bypass Rust compiler checks can severely degrade concurrency safety of Rust programs. 22 of them synchronize their shared memory accesses, but there are issues in the synchronization. For example, expected atomicity is not achieved or expected access order is violated.

Insight 8: *How data is shared is not necessarily associated with how non-blocking bugs happen, and the former can be in unsafe code and the latter can be in safe code.*

There are seven bugs involving Rust-unique libraries, including two related to message passing. When multiple threads request mutable references of a `RefCell` at the same time, a runtime panic will be triggered. This is the root cause of four bugs. A buggy `RefCell` is shared using `Sync` trait for two of them and using pointers for the other two. Rust provides a unique strategy where a mutex is poisoned when a thread holding the mutex panics. Another thread waiting for the mutex will receive `Err` from `Lock()`. The poisoning mechanism allows panic information to be propagated across threads. One bug is caused by failing to send out a logging message when poisoning happens. The other two bugs are caused by panics when misusing `Arc` or channel.

Insight 9: *Misusing Rust's unique libraries is one major root cause of non-blocking bugs, and all these bugs are captured by runtime checks inside the libraries, demonstrating the effectiveness of Rust's runtime checks.*

Interior Mutability. As explained in Section 2.3, interior mutability is a pattern where a function internally mutates values, but these values look immutable from outside the

```
1  impl Engine for AuthorityRound {
2    fn generate_seal(&self) -> Seal {
3  -   if self.proposed.load() { return Seal::None; }
4  -   self.proposed.store(true);
5  -   return Seal::Regular(...);
6  +   if !self.proposed.compare_and_swap(false, true) {
7  +     return Seal::Regular(...);
8  +   }
9  +   return Seal::None;
10   }
```

Figure 7. A non-blocking bug in Ethereum.

function. Improper use of interior mutability can cause non-blocking bugs (14 in total in our studied set).

Figure 7 shows one such example. `AuthorityRound` is a struct that implements the `Sync` trait (thus an `AuthorityRound` object can be shared by multiple threads after declared with `Arc`). The field `proposed` is an atomic boolean variable, initialized as `false`. The intention of the `generate_seal()` function is to return a `Seal` object only once at a time, and the programmers (improperly) used the `proposed` field in lines 3 and 4 to achieve this goal. When two threads call `generate_seal()` on the same object and both of them finish executing line 3 before executing line 4, both threads will get a `Seal` object as the function return value, violating the program's intended goal. The patch is to use an atomic instruction at line 6 to replace lines 3 and 4.

In this buggy code, the `generate_seal()` function modifies the immutably borrowed parameter `&self` by changing the value of the `proposed` field. If the function's input parameter is set as `&mut self` (mutable borrow), the Rust compiler would report an error when the invocation of `generate_seal()` happens without holding a lock. In other words, if programmers use mutable borrow, then they would have avoided the bug with the help of the Rust compiler. There are 13 more non-blocking bugs in our collected bug set where the shared object `self` is immutably borrowed by a struct function but is changed inside the function. For five of them, the object (`self`) is shared safely. The Rust compiler would have reported errors if these borrow cases were changed to mutable.

Rust programmers should carefully design interfaces (*e.g.*, mutable borrow vs. immutable borrow) to avoid non-blocking bugs. With proper interfaces, the Rust compiler would be able to enable more checks, which could report potential bugs.

Insight 10: *The design of APIs can heavily impact the Rust compiler's capability of identifying bugs.*

Suggestion 8: *Internal mutual exclusion must be carefully reviewed for interior mutability functions in structs implementing `Sync` trait.*

Fixes of Non-Blocking Bugs. The fixing strategies of our studied Rust bugs are similar to those in other programming languages [31, 70]. 19 bugs are fixed by adjusting synchronization primitives to enforce atomic accesses to shared memory. Nine are fixed by enforcing ordering between two shared-memory accesses from different threads. Five are fixed by avoiding (problematic) shared memory accesses. One is fixed by making a local copy of some shared memory. Finally, three are fixed by changing application-specific logic.

Insight 11: *Fixing strategies of Rust non-blocking (and blocking) bugs are similar to traditional languages. Existing automated bug fixing techniques are likely to work on Rust too.*

7 Bug Detection

Our empirical bug study reveals that Rust's compiler checks fail to cover many types of bugs. We believe that Rust bug detection tools should be developed and our study results can greatly help these developments. Unfortunately, existing Rust bug detectors (Section 2.4) are far from sufficient. From our experiments, the Rust-clippy detector failed to detect any of our collected bugs. The Miri dynamic detector can only report bugs when a test run happens to trigger problematic execution. Moreover, it has many false positive bug reports. Rust's debug mode can help detect double locks and integer overflows. But similar to Miri, it also needs a test input to trigger buggy execution.

This section discusses how our bug study results can be used to develop bug detection tools. We also present two new bug detectors we built for statically detecting Rust use-after-free and double-lock bugs. Note that although the results of these bug detectors are promising, they are just our initial efforts in building Rust bug detectors. We encourage researchers and practitioners to invest more on Rust bug detection based on our initial results.

7.1 Detecting Memory Bugs

From our study of memory bugs, we found that many memory-related issues are caused by misuse of ownership and lifetime. Thus, an efficient way to avoid or detect memory bugs in Rust is to analyze object ownership and lifetime.

IDE tools. Misunderstanding Rust's ownership and lifetime rules is common (because of the complexity of these rules when used in real-world software), and it is the main cause of memory bugs. Being able to visualize objects' lifetime and owner(s) during programming time could largely help Rust programmers *avoid* memory bugs. An effective way of visualization is to add plug-ins to IDE tools, for example, by highlighting a variable's lifetime scope when the mouse/cursor hops over it or its pointer/reference. Programmers can easily notice errors when a pointer's usage is outside the lifetime of the object it points to and avoid a use-after-free bug. Highlighting and annotating ownership operations can also help programmers avoid various memory bugs such as double-free bugs and invalid-free bugs (*e.g.*, Figure 4).

Static detectors. Ownership/lifetime information can also be used to statically detect memory bugs. Based on our study results in Section 5, it is feasible to build static checkers to detect invalid-free, use-after-free, double-free memory bugs

by analyzing object lifetime and ownership relationships. For example, at the end of an object's lifetime, we can examine whether or not this object has been correctly initialized to detect invalid-free bugs like Figure 4.

As a more concrete example, we have built a new static checker based on lifetime/ownership analysis of Rust's mid-level intermediate representation (MIR) to detect use-after-free bugs like Figure 5. We chose MIR to perform the analysis because it provides explicit ownership/lifetime information and rich type information. Our detector maintains the state of each variable (*alive* or *dead*) by monitoring when MIR calls `StorageLive` or `StorageDead` on the variable. For each pointer/reference, we conduct a "points-to" analysis to maintain which variable it points to/references. This points-to analysis also includes cases where the ownership of a variable is moved. When a pointer/reference is dereferenced, our tool checks if the object it points to is dead and reports a bug if so.

In total, our detector found four previously unknown bugs in our studied applications. Our tool currently reports three false positives, all caused by our current (unoptimized) way of performing inter-procedural analysis. We leave improving inter-procedural analysis to future work.

Overall, the results of our initial efforts in building static bug detectors are encouraging, and they confirm that ownership/lifetime information is useful in detecting memory bugs that cannot be reported by the Rust compiler.

Dynamic detectors. Apart from IDE tools and static bug detectors, our study results can also be used to build or improve dynamic bug detectors. Fuzzing is a widely-used method to detect memory bugs in traditional programming languages [1, 5, 49, 61, 74, 77]. Our study in Section 5 finds that all Rust memory bugs (after the Rust language has been stabilized in 2016) involve unsafe code. Instead of blindly fuzzing all code, we recommend future fuzzing tools to focus on unsafe code and its related safe code to improve the performance of fuzzing.

7.2 Detecting Concurrency Bugs

There are many ways to use our study results of concurrency bugs in Section 6 to build concurrency bug detectors. We now discuss how our results can be used and a real static double-lock detector we built.

IDE tools. Rust's implicit lock release is the cause of several types of blocking bugs such as the double-lock bug in Figure 6. An effective way to avoid these bugs is to visualize critical sections. The boundary of a critical section can be determined by analyzing the lifetime of the return of the function `Lock`. Highlighting blocking operations such as `Lock` and channel-receive inside a critical section is also a good way to help programmers avoid blocking bugs.

IDE tools can also help avoid non-blocking bugs. For example, to avoid bugs caused by improper use of interior mutability, we can annotate the call sites of interior mutable functions and remind developers that these functions will change their immutably borrowed parameters.

Static detectors. Lifetime and ownership information can be used to statically detect blocking bugs. We built a double-lock detector by analyzing lock lifetime. It first identifies all call sites of `Lock` (or `RwLock`) and extracts two pieces of information from each call site: the lock being acquired and the variable being used to save the return value. As Rust implicitly releases the lock when the lifetime of this variable ends, our tool will record this release time. We then check whether or not the same lock is acquired before this time, and report a double-lock bug if so. Our check covers the case where two lock acquisitions are in different functions by performing inter-procedural analysis. Our detector has identified six previously unknown double-lock bugs in our studied applications (and no false positives). They have been fixed by developers after we reported them.

Ownership information can also help static detections of non-blocking bugs. For example, for bugs caused by misuse of interior mutability like the one in Figure 7, we could perform the following static check. When a `struct` is sharable (*e.g.*, implementing the `Sync` trait) and has a method immutably borrowing `self`, we can analyze whether `self` is modified in the method and whether the modification is unsynchronized. If so, we can report a potential bug. On the other hand, we do not need to analyze a function that mutably borrows `self`, since the Rust compiler will enforce the function to be called with a lock, guaranteeing the proper synchronization of its internal operations.

Dynamic detectors. Dynamic concurrency-bug detectors often have the need to track shared variable accesses. Being able to differentiate thread-local variables from shared variables can help lower memory and runtime overhead of dynamic bug detectors' tracking. Our empirical study results identify the (limited) code patterns of data sharing across threads in Rust. Dynamic detectors can use these patterns to reduce the amount of tracking to only shared variables.

8 Conclusion

As a programming language designed for safety, Rust provides a suite of compiler checks to rule out memory and thread safety issues. Facing the increasing adoption of Rust in mission-critical systems like OSes and browsers, this paper conducts the first comprehensive, empirical study on unsafe usages, memory bugs and concurrency bugs in real-world Rust programs. Many insights and suggestions are provided in our study. We expect our study to deepen the understanding of real-world safety practices and safety issues in Rust and guide the programming and research tool design of Rust.

References

[1] AFL. 2019. American fuzzy lop. http://lcamtuf.coredump.cx/afl/.

[2] Marek Baranowski, Shaobo He, and Zvonimir Rakamarić. 2018. Verifying Rust Programs with SMACK. In *Automated Technology for Verification and Analysis (ATVA '18)*. Los Angeles, CA.

[3] Kevin Boos and Lin Zhong. 2017. Theseus: A State Spill-free Operating System. In *Proceedings of the 9th Workshop on Programming Languages and Operating Systems (PLOS '17)*. Shanghai, China.

[4] Cristian Cadar, Daniel Dunbar, and Dawson Engler. 2008. KLEE: Unassisted and Automatic Generation of High-coverage Tests for Complex Systems Programs. In *Proceedings of the 8th USENIX Conference on Operating Systems Design and Implementation (OSDI '08)*. Berkeley, CA, USA.

[5] Peng Chen and Hao Chen. 2018. Angora: Efficient Fuzzing by Principled Search. *Proceedings of the 39th IEEE Symposiums on Security and Privacy (Oakland '18)* (2018).

[6] Lee Chew and David Lie. 2010. Kivati: Fast Detection and Prevention of Atomicity Violations. In *Proceedings of the 5th European Conference on Computer systems (EuroSys '10)*. Paris, France.

[7] Andy Chou, Junfeng Yang, Benjamin Chelf, Seth Hallem, and Dawson Engler. 2001. An Empirical Study of Operating Systems Errors. In *Proceedings of the 18th ACM symposium on Operating Systems Principles (SOSP '01)*. Banff, Canada.

[8] Yong Wen Chua. 2017. Appreciating Rust's Memory Safety Guarantees. https://blog.gds-gov.tech/appreciating-rust-memory-safety-438301fee097

[9] Catalin Cimpanu. 2019. Microsoft to explore using Rust. https://www.zdnet.com/article/microsoft-to-explore-using-rust

[10] Crossbeam. 2019. Tools for concurrent programming in Rust. https://github.com/crossbeam-rs/crossbeam

[11] Weidong Cui, Xinyang Ge, Baris Kasikci, Ben Niu, Upamanyu Sharma, Ruoyu Wang, and Insu Yun. 2018. REPT: Reverse Debugging of Failures in Deployed Software. In *Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation (OSDI '18)*. Carlsbad, CA.

[12] CVE. 2019. Common Vulnerabilities and Exposures. https://cve.mitre.org/cve/

[13] Kyle Dewey, Jared Roesch, and Ben Hardekopf. 2015. Fuzzing the Rust Typechecker Using CLP (T). In *Proceedings of the 2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE '15)*. Lincoln, NE.

[14] John Erickson, Madanlal Musuvathi, Sebastian Burckhardt, and Kirk Olynyk. 2010. Effective Data-race Detection for the Kernel. In *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI '10)*. Vancouver, Canada.

[15] Ethereum. 2019. The Ethereum Project. https://www.ethereum.org/

[16] Firecracker. 2019. Secure and fast microVMs for serverless computing. https://firecracker-microvm.github.io/

[17] Cormac Flanagan and Stephen N Freund. 2004. Atomizer: A Dynamic Atomicity Checker for Multithreaded Programs. In *Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of programming languages (POPL '04)*. Venice, Italy.

[18] Qi Gao, Wenbin Zhang, Zhezhe Chen, Mai Zheng, and Feng Qin. 2011. 2ndStrike: Toward Manifesting Hidden Concurrency Typestate Bugs. In *Proceedings of the 16th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '11)*. Newport Beach, CA.

[19] Rui Gu, Guoliang Jin, Linhai Song, Linjie Zhu, and Shan Lu. 2015. What Change History Tells Us About Thread Synchronization. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*. Bergamo, Italy.

[20] Haryadi S. Gunawi, Mingzhe Hao, Tanakorn Leesatapornwongsa, Tiratat Patana-anake, Thanh Do, Jeffry Adityatama, Kurnia J. Eliazar, Agung Laksono, Jeffrey F. Lukman, Vincentius Martin, and Anang D. Satria. 2014. What Bugs Live in the Cloud? A Study of 3000+ Issues in Cloud Systems. In *Proceedings of the ACM Symposium on Cloud Computing (SOCC' 14)*. Seattle, WA.

[21] Jeff Huang. 2016. Scalable Thread Sharing Analysis. In *Proceedings of the 38th International Conference on Software Engineering (ICSE '16)*. New York, NY, USA.

[22] IotEdge. 2019. IoT Edge Security Daemon. https://github.com/Azure/iotedge/tree/master/edgelet

[23] Guoliang Jin, Linhai Song, Xiaoming Shi, Joel Scherpelz, and Shan Lu. 2012. Understanding and Detecting Real-world Performance Bugs. In *Proceedings of the 33rd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI' 12)*. Beijing, China.

[24] Ralf Jung, Jacques-Henri Jourdan, Robbert Krebbers, and Derek Dreyer. 2018. RustBelt: Securing the Foundations of the Rust Programming Language. In *Proceedings of the 45th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL '18)*. Los Angeles, CA.

[25] Shuanglong Kan, David Sanán, Shang-Wei Lin, and Yang Liu. 2018. K-Rust: An Executable Formal Semantics for Rust. *CoRR* (2018).

[26] Chris Lattner and Vikram Adve. 2004. LLVM: A Compilation Framework for Lifelong Program Analysis & Transformation. In *Proceedings of the International Symposium on Code Generation and Optimization (CGO '04')*. Washington, DC, USA.

[27] Lazy-static. 2019. A macro for declaring lazily evaluated statics in Rust. https://github.com/rust-lang-nursery/lazy-static.rs

[28] Tanakorn Leesatapornwongsa, Jeffrey F. Lukman, Shan Lu, and Haryadi S. Gunawi. 2016. TaxDC: A Taxonomy of Non-Deterministic Concurrency Bugs in Datacenter Distributed Systems. In *Proceedings of the 21th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '16)*. Atlanta, GA.

[29] Amit Levy, Bradford Campbell, Branden Ghena, Daniel B. Giffin, Pat Pannuto, Prabal Dutta, and Philip Levis. 2017. Multiprogramming a 64kB Computer Safely and Efficiently. In *Proceedings of the 26th Symposium on Operating Systems Principles (SOSP '17)*. Shanghai, China.

[30] Ziyi Lin, Darko Marinov, Hao Zhong, Yuting Chen, and Jianjun Zhao. 2015. JaConTeBe: A Benchmark Suite of Real-World Java Concurrency Bugs. In *30th IEEE/ACM International Conference on Automated Software Engineering (ASE '15)*. Lincoln, NE.

[31] Haopeng Liu, Yuxi Chen, and Shan Lu. 2016. Understanding and Generating High Quality Patches for Concurrency Bugs. In *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE '16)*. Seattle, WA.

[32] Lanyue Lu, Andrea C. Arpaci-Dusseau, Remzi H. Arpaci-Dusseau, and Shan Lu. 2013. A Study of Linux File System Evolution. In *Proceedings of the 11th USENIX Conference on File and Storage Technologies (FAST '13)*. San Jose, CA.

[33] Shan Lu, Soyeon Park, Eunsoo Seo, and Yuanyuan Zhou. 2008. Learning from mistakes – A comprehensive study of real world concurrency bug characteristics. In *Proceedings of the 13th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '08)*. Seattle, WA.

[34] Shan Lu, Joseph Tucek, Feng Qin, and Yuanyuan Zhou. 2006. AVIO: Detecting Atomicity Violations via Access Interleaving Invariants. In *Proceedings of the 12th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '06)*. San Jose, CA.

[35] Brandon Lucia and Luis Ceze. 2009. Finding Concurrency Bugs with Context-aware Communication Graphs. In *Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO '09)*. New York, NY.

[36] Ricardo Martins. 2016. Interior mutability in Rust, part 2: thread safety. https://ricardomartins.cc/2016/06/25/interior-mutability-thread-safety

[37] Miri. 2019. *An interpreter for Rust's mid-level intermediate representation*. https://github.com/rust-lang/miri

[38] MSRC. 2019. Why Rust for safe systems programming. https://msrc-blog.microsoft.com/2019/07/22/why-rust-for-safe-systems-programming

[39] Octoverse. 2019. The State of Octoverse. https://octoverse.github.com/

[40] Stack Overflow. 2016. Stack Overflow Developer Survey 2016. https://insights.stackoverflow.com/survey/2016#technology-most-loved-dreaded-and-wanted

[41] Stack Overflow. 2017. Stack Overflow Developer Survey 2017. https://insights.stackoverflow.com/survey/2017#most-loved-dreaded-and-wanted

[42] Stack Overflow. 2018. Stack Overflow Developer Survey 2018. https://insights.stackoverflow.com/survey/2018/#most-loved-dreaded-and-wanted

[43] Stack Overflow. 2019. Stack Overflow Developer Survey 2019. https://insights.stackoverflow.com/survey/2019#most-loved-dreaded-and-wanted

[44] Alex Ozdemir. 2019. Unsafe in Rust: Syntactic Patterns. https://cs.stanford.edu/~aozdemir/blog/unsafe-rust-syntax

[45] Alex Ozdemir. 2019. Unsafe in Rust: The Abstraction Safety Contract and Public Escape. https://cs.stanford.edu/~aozdemir/blog/unsafe-rust-escape

[46] Parity-ethereum. 2019. The Parity Ethereum Client. https://www.parity.io/ethereum/

[47] Quantum. 2019. Quantum. https://wiki.mozilla.org/Quantum

[48] Rand. 2019. Rand. A Rust library for random number generation. https://github.com/rust-random/rand

[49] Sanjay Rawat, Vivek Jain, Ashish Kumar, Lucian Cojocar, Cristiano Giuffrida, and Herbert Bos. 2017. VUzzer: Application-aware Evolutionary Fuzzing. In *Proceedings of the 2017 Annual Network and Distributed System Security Symposium (NDSS '17)*. San Diego, CA, USA.

[50] Rayon. 2019. A data parallelism library for Rust. https://github.com/rayon-rs/rayon

[51] Redox. 2019. The Redox Operating System. https://www.redox-os.org/

[52] Eric Reed. 2015. *Patina: A Formalization of the Rust Programming Language*. Technical Report UW-CSE-15-03-02. University of Washington.

[53] Rust-book. 2019. Fearless Concurrency. https://doc.rust-lang.org/book/ch16-00-concurrency.html

[54] Rust-book. 2019. Validating References with Lifetimes. https://doc.rust-lang.org/book/ch10-03-lifetime-syntax.html

[55] Rust-clippy. 2019. A bunch of lints to catch common mistakes and improve your Rust code. https://github.com/rust-lang/rust-clippy

[56] Rust-nomicon. 2019. The Rustonomicon. https://doc.rust-lang.org/nomicon/

[57] RustSec. 2019. Security advisory database for Rust crates. https://github.com/RustSec/advisory-db

[58] Stefan Savage, Michael Burrows, Greg Nelson, Patrick Sobalvarro, and Thomas Anderson. 1997. Eraser: A Dynamic Data Race Detector for Multithreaded Programs. *ACM Transactions on Computer Systems, 15(4):391-411* (1997).

[59] Servo. 2019. The Servo Browser Engine. https://servo.org/

[60] Sid Shanker. 2018. Safe Concurrency with Rust. http://squidarth.com/rc/rust/2018/06/04/rust-concurrency.html

[61] Nick Stephens, John Grosen, Christopher Salls, Andrew Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. 2016. Driller: Augmenting Fuzzing Through Selective Symbolic Execution. In *Proceedings of the 2016 Annual Network and Distributed System Security Symposium (NDSS '16)*. San Diego, CA, USA.

[62] Straits. 2019. Stratis: Easy to use local storage management for Linux. https://stratis-storage.github.io/

[63] Mingshen Sun, Yulong Zhang, and Tao Wei. 2018. When Memory-Safe Languages Become Unsafe. In *DEF CON China (DEF CON China '18')*. Beijing, China.

[64] Benchmarks Game Team. 2019. Rust versus C gcc fastest programs. https://benchmarksgame-team.pages.debian.net/benchmarksgame/faster/rust.html

[65] The Rust Team. 2019. Rust Empowering everyone to build reliable and efficient software. https://www.rust-lang.org/

[66] Threadpool. 2019. A very simple thread pool for parallel task execution. https://github.com/rust-threadpool/rust-threadpool

[67] Tikv. 2019. A distributed transactional key-value database. https://tikv.org/

[68] Tock. 2019. Tock Embedded Operating System. https://www.tockos.org/

[69] Tock. 2019. unnecessary unsafe tag. Tock issue #1298. https://github.com/tock/tock/issues/1298

[70] Tengfei Tu, Xiaoyu Liu, Linhai Song, and Yiying Zhang. 2019. Understanding Real-World Concurrency Bugs in Go. In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '19)*. Providence, RI.

[71] Wikipedia. 2019. Rust (programming language). https://en.wikipedia.org/wiki/Rust_(programming_language)

[72] Jun Xu, Dongliang Mu, Ping Chen, Xinyu Xing, Pei Wang, and Peng Liu. 2016. CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core Dump. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Vienna, Austria.

[73] Jun Xu, Dongliang Mu, Xinyu Xing, Peng Liu, Ping Chen, and Bing Mao. 2017. POMP: Postmortem Program Analysis with Hardware-enhanced Post-crash Artifacts. In *Proceedings of the 26th USENIX Conference on Security Symposium (Security '17)*. Vancouver, Canada.

[74] Wei You, Xueqiang Wang, Shiqing Ma, Jianjun Huang, Xiangyu Zhang, Xiaofeng Wang, and Bin Liang. 2019. ProFuzzer: On-the-fly Input Type Probing for Better Zero-Day Vulnerability Discovery. In *Proceedings of the 40th IEEE Symposiums on Security and Privacy (Oakland '19)*.

[75] Jie Yu and Satish Narayanasamy. 2009. A Case for an Interleaving Constrained Shared-memory Multi-processor. In *Proceedings of the 36th annual International symposium on Computer architecture (ISCA '09)*. Austin, TX.

[76] Yuan Yu, Tom Rodeheffer, and Wei Chen. 2005. RaceTrack: Efficient Detection of Data Race Conditions via Adaptive Tracking. In *Proceedings of the 20th ACM symposium on Operating systems principles (SOSP '05)*. Brighton, United Kingdom.

[77] Insu Yun, Sangho Lee, Meng Xu, Yeongjin Jang, and Taesoo Kim. 2018. QSYM: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing. In *Proceedings of the 27th USENIX Conference on Security Symposium (Usenix Security '18)*. Berkeley, CA, USA.

[78] Wei Zhang, Junghee Lim, Ramya Olichandran, Joel Scherpelz, Guoliang Jin, Shan Lu, and Thomas Reps. 2011. ConSeq: Detecting Concurrency Bugs Through Sequential Errors. In *Proceedings of the Sixteenth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '11)*. New York, NY, USA.

[79] Wei Zhang, Chong Sun, and Shan Lu. 2010. ConMem: detecting severe concurrency bugs through an effect-oriented approach. In *Proceedings of the 15th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '10)*. Pittsburgh, PA.