KARD: Lightweight Data Race Detection with Per-Thread Memory Protection

Adil Ahmad
Purdue University, USA

Pedro Fonseca
Purdue University, USA

Sangho Lee
Microsoft Research, USA

Byoungyoung Lee
Seoul National University, South Korea

ABSTRACT
Finding data race bugs in multi-threaded programs has proven challenging. A promising direction is to use dynamic detectors that monitor the program’s execution for data races. However, despite extensive work on dynamic data race detection, most proposed systems for commodity hardware incur prohibitive overheads due to expensive compiler instrumentation of memory accesses; hence, they are not efficient enough to be used in all development and testing settings.

KARD is a lightweight system that dynamically detects data races caused by inconsistent lock usage—when a program concurrently accesses the same memory object using different locks or only some of the concurrent accesses are synchronized using a common lock. Unlike existing detectors, KARD does not monitor memory accesses using expensive compiler instrumentation. Instead, KARD leverages commodity per-thread memory protection, Intel Memory Protection Keys (MPK). Using MPK, KARD ensures that a shared object is only accessible to a single thread in its critical section, and captures all violating accesses from other concurrent threads. KARD overcomes various limitations of MPK by introducing key-enforced race detection, employing consolidated unique page allocation, carefully managing protection keys, and automatically pruning out non-racy or redundant violations. Our evaluation shows that KARD detects all data races caused by inconsistent lock usage and has a low geometric mean execution time overhead: 7.0% on PARSEC and SPLASH-2x benchmarks and 5.3% on a set of real-world applications (NGINX, memcached, pigz, and Aget).

CCS CONCEPTS

KEYWORDS
concurrency, data race, lock, memory protection keys

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 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.

ASPLOS ’21, April 19–23, 2021, Virtual, USA
© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8317-2/21/04...$15.00
https://doi.org/10.1145/3445814.3446727

1 INTRODUCTION
Dynamic data race detectors find real-world data races with low false positives [58], but generally incur prohibitive performance overheads. For example, the state-of-the-art dynamic data race detector, Google’s ThreadSanitizer (TSan) [52], employs compiler-based memory access instrumentation that slows down program execution by almost 7×. Due to its prohibitive overhead, TSan is not applicable to all development or testing settings [34].

Unfortunately, existing approaches to improve the performance of data race detection have seen limited adoption due to their deployment and effectiveness limitations. Some schemes require system software modifications [42, 64], hardware modifications [38, 65] or extensive developer effort [21, 64], which hinder deployability. Others employ sampling [13, 20, 53, 63] that results in probabilistic guarantees and needs to be calibrated with a low sampling rate, hence low effectiveness, to ensure adequate performance.

This paper proposes KARD, a low-overhead yet practical dynamic data race detector that does not require hardware or system software changes, developer effort, and sampling. KARD detects data races due to inconsistent lock usage [28] that occurs when a program concurrently accesses the same memory object using different locks or only some of the concurrent accesses are synchronized using a common lock. Our analysis of fixed real-world data races detected by TSan shows that inconsistent lock usage constitutes approximately 69% of all reported data races (§3.1). Furthermore, under the standard testing scenario of 4 threads [36], KARD incurs a performance overhead of only 5.3% across a range of real-world applications. Hence, KARD is an effective data race detection tool that is applicable in many testing and development settings.

We introduce a novel data race detection algorithm based on the concept of key-enforced access (§4). KARD uses this algorithm to detect data races caused by inconsistent lock usage. In particular, key-enforced access protects each shared object accessed in a lock-protected code region (i.e., a critical section) using a key. While a thread holds a shared object’s key within a critical section, all conflicting concurrent access (with a different lock or without a lock) to the object is flagged as a data race.
KARD implements the algorithm efficiently by leveraging Intel’s Memory Protection Keys (MPK) [14], a hardware feature available on commodity CPUs [1, 39]. MPK allows software to change each thread’s page access permissions by modifying a thread-local register (PKRU) with a non-privileged instruction (WRPKRU). Importantly, updating PKRU does not flush the Translation Lookaside Buffer (TLB); hence, updating memory protection using MPK is very efficient, as noted by other studies [26, 43, 57].

Nevertheless, KARD must overcome three important challenges including those presented by the hardware limitations of MPK. First, KARD must protect individual shared objects instead of memory pages, the minimum unit of MPK protection, potentially containing multiple shared objects. Third, KARD must concurrently monitor many threads and objects, even though MPK only provides a limited number of protection keys.

To overcome these challenges, KARD implements (a) an automated scheme that identifies shared objects accessed in critical sections by trapping access on them using memory protection (§5.3), (b) a consolidated unique page allocation scheme that assigns unique virtual pages to each memory object and ensures a low memory footprint using virtual page consolidation techniques (§5.3), and (c) an effective key assignment scheme that reuses keys within critical sections to ensure that KARD seldom runs out of protection keys (§5.4).

Furthermore, KARD dynamically analyzes all MPK-driven access violations (General Protection Fault (#GP)) raised by the program to prune out redundant or spurious faults. In particular, KARD uses a new technique to prune spurious faults, protection interleaving, that can detect byte-level access made by each thread and test the validity of raised warnings (§5.5).

We implement KARD using an LLVM compiler pass to trap heap allocation and synchronization calls, and a C++-based runtime library that creates unique paged heap objects and assigns protection to a group of memory pages [14]. MPK currently supports up to 16 protection keys (k0 to k15), which are assigned to memory pages through pkey_mprotect() system calls. However, since the first key (k0) is reserved for backward compatibility, the effective number of available keys is 15.

With MPK, each thread can configure its access to memory pages protected by a certain protection key via a thread-local register, PERU. In particular, MPK provides two non-privileged instructions, RDPKRU and WRPKRU, to allow the thread to retrieve and update its PERU, respectively. These instructions are fast: RDPKRU takes less than 1 cycle and WRPKRU takes around 20 cycles [43]. The main reason behind their efficiency is that they do not change page table entries or require a TLB flush unlike mprotect().

<table>
<thead>
<tr>
<th>Concurrent access to the same object</th>
<th>ILU</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1</td>
<td>t2</td>
</tr>
<tr>
<td>With lock k0</td>
<td>With lock k0</td>
</tr>
<tr>
<td>With lock k0</td>
<td>No lock</td>
</tr>
<tr>
<td>No lock</td>
<td>With lock k0</td>
</tr>
<tr>
<td>No lock</td>
<td>No lock</td>
</tr>
</tbody>
</table>

Table 1: Inconsistent lock usage (ILU) between concurrent accesses to the same object by two different threads t1 and t2 (✓: in scope, x: out of scope). a way that they can be executed simultaneously on a multi-core machine, and at least one of the accesses is a write.

**Lock.** A lock is a programming abstraction that allows a thread to synchronize the execution of its code with other concurrent threads. At a lock acquisition site, a thread stalls its execution if the lock is exclusively held by another thread.

**Critical section.** A critical section is a code region between lock and unlock functions. Even if the program can acquire different sets of locks on a given code region, we still consider it a single critical section.

**Sharable object.** A sharable object is any heap or global object in a program, accessible to any executing program thread.

**Shared object.** A shared object is any sharable object accessed within a critical section.

### 2.2 Intel Memory Protection Keys (MPK)

Intel MPK is a CPU extension for per-thread memory protection that assigns either no access, read-only, or read-write permissions to a group of memory pages [14]. MPK currently supports up to 16 different protection keys (k0 to k15), which are assigned to memory pages through pkey_mprotect() system calls. However, since the first key (k0) is reserved for backward compatibility, the effective number of available keys is 15.

With MPK, each thread can configure its access to memory pages protected by a certain protection key via a thread-local register, PERU. In particular, MPK provides two non-privileged instructions, RDPKRU and WRPKRU, to allow the thread to retrieve and update its PERU, respectively. These instructions are fast: RDPKRU takes less than 1 cycle and WRPKRU takes around 20 cycles [43]. The main reason behind their efficiency is that they do not change page table entries or require a TLB flush unlike mprotect().

### 3 MOTIVATION AND GOAL

This section explains the significance of inconsistent lock usage in real-world data races, explains the limitation of existing detection schemes, and defines our goal.

#### 3.1 Inconsistent Lock Usage

Inconsistent lock usage (ILU) refers to scenarios where a program’s threads concurrently access the same memory object using different locks or only some of the accesses are synchronized using a common lock [28]. Table 1 illustrates ILU’s scope. Specifically, two threads...
concurrently access the same shared object while holding different locks, \( L_a \) or \( L_b \), or only one of them acquires either \( L_a \) or \( L_b \).

ILU is inspired by the traditional lockset algorithm \([49]\), but considers concurrency to ignore many scenarios where lockset reports false data race warnings. In particular, lockset assumes that if an access to a shared object is using a set of locks that is inconsistent (i.e., no common lock) with a previous access to the object, it can result in a data race. However, lockset is agnostic to whether the two accesses can concurrently occur or not. Hence, in practice, lockset falsely reports many instances that do not result in a data race.

In contrast to lockset’s scope, ILU is aware of concurrently executing threads; thus, it is more precise in relation to instances that might result in a data race. However, ILU is schedule-sensitive, i.e., the threads must be scheduled in a way that results in inconsistent lock usage, unlike lockset. We believe that such a trade-off is essential because a schedule-sensitive scope mitigates instances of chasing false bugs in development and testing settings, which are especially undesirable \([34, 48]\). Furthermore, as long as the tool employing such a scope is lightweight, it can be utilized under many test cases to detect data races in diverse code regions, unlike the expensive schedule-insensitive lockset.

Data races due to ILU scenarios are very common in real-world applications: our analysis shows that the majority of data races, reported by TSan \([52]\), in real-world applications are associated with ILU. We analyzed real-world data races found by TSan that were eventually fixed \([58]\), to filter out potential benign or intentional data races. We randomly chose 100 fixed bug reports for which we could find attached TSan logfiles (stacktraces of execution), and manually investigated them. We confirmed that 69% of them were involved ILU; that is, at least one of the conflicting threads in each report was holding a lock.

Note that TSan might be biased in its reported data races. This potential bias reflects a general limitation of real-world application bug studies caused by the difficulty to analyze the entire population of both identified and unidentified bugs \([22, 24]\). We chose TSan because it is the state-of-the-art in dynamic data race detection and continuously finds critical bugs in real-world applications. Furthermore, TSan maintains a robust and verifiable bug database. In this regard, our analysis on TSan’s reported bugs empirically shows that many real-world data race bugs can be classified under ILU.

### 3.2 Limitations of Existing Approaches

Existing systems \([9, 13, 18, 20, 37, 38, 42, 52, 62, 64, 65]\) detect data races due to ILU or more, but have various performance, deployment, usability, or scope limitations. Table 2 illustrates the characteristics of existing approaches.

#### Expensive memory instrumentation.

Systems like TSan \([52]\) and TxRace \([62]\) employ compiler instrumentation of all or partial memory accesses, allowing them to report a large class of data races, but with prohibitive performance costs (i.e., \(7x\) for TSan and \(5x\) for TxRace under 4 threads). A recent study \([34]\) shows that such overheads hinder their adoption in many development or testing scenarios.

### Table 2: Comparison between Kard and existing approaches. Requirements include expensive memory instrumentation (MI), system (software or hardware) change (SC), and developer effort (DE) (\(\bigcirc\): required, \(\bigcirc\): not required). Scope includes inconsistent lock usage (ILU) and inconsistent lock usage and others (ILU+).

<table>
<thead>
<tr>
<th>System</th>
<th>Requirements</th>
<th>Scope</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eraser ([49])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>Very high</td>
</tr>
<tr>
<td>Inspector XE ([12])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>Very high</td>
</tr>
<tr>
<td>TSan ([52])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>Very high</td>
</tr>
<tr>
<td>Valor ([9])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>High</td>
</tr>
<tr>
<td>Custom Hardware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HARD ([65])</td>
<td>(\bigcirc)</td>
<td>ILU</td>
<td>Low</td>
</tr>
<tr>
<td>Conflict Exception ([38])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>Low</td>
</tr>
<tr>
<td>Probabilistic Sampling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DataCollider ([20])</td>
<td>(\bigcirc)</td>
<td>Sampled (ILU+)</td>
<td>Moderate/low/moderate</td>
</tr>
<tr>
<td>Pacer ([13])</td>
<td>(\bigcirc)</td>
<td>Sampled (ILU+)</td>
<td>Moderate/high</td>
</tr>
<tr>
<td>Memory Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aikido ([42])</td>
<td>(\bigcirc)</td>
<td>ILU+</td>
<td>Very high</td>
</tr>
<tr>
<td>PUSH ([64])</td>
<td>(\bigcirc)</td>
<td>ILU</td>
<td>Low</td>
</tr>
<tr>
<td>KARD (our work)</td>
<td>(\bigcirc)</td>
<td>ILU</td>
<td>Low</td>
</tr>
</tbody>
</table>

#### System changes.

Other schemes improve the performance of race detection by proposing system changes in the form of (a) hardware modifications \([38, 65]\) or (b) software modifications to the OS \([64]\) or hypervisor \([42]\). These suffer from deployment problems because custom hardware is nontrivial to manufacture and system software changes are less feasible in many environments (e.g., VM or container instances).

#### Developer efforts.

Another approach to improve data race detection performance is selectively monitoring shared objects manually annotated by developers. However, given the challenges of manual annotation, adoption of such schemes is less likely to occur in practice. For example, PUSH \([64]\), a scheme involving such developer effort, required 35 hours for annotation on a benchmark application (i.e., streamcluster \([8]\)).

#### Probabilistic protection scope.

Sampling techniques improve the performance of data race detectors by monitoring a small subset of instructions \([13]\) or objects \([20]\) at a time. However, low sampling rates for good performance yield low probabilistic effectiveness.

### 3.3 Goal

Motivated by the significance of data races due to ILU \((3.1)\) and the limitations of existing work \((3.2)\), we intend to design a novel data race detector, specifically for ILU data races, that satisfies the following goals.

- **Lightweight:** No individual memory access instrumentation
- **Deployable:** Neither hardware nor system software changes
- **Automated:** No manual annotation
- **Systematic:** No sampling
4 KEY-ENFORCED RACE DETECTION

This section introduces an algorithm based on the concept of key-enforced access to detect race data due to ILU. With key-enforced access, each shared object accessed in critical sections is protected by a key. A thread that enters a critical section can acquire a key to access a shared object and, later, the thread releases the acquired key when it exits the critical section.

Key-enforced access further distinguishes read-only keys from read-write keys to fulfill the concept of shared read and exclusive write. In particular, a thread can acquire a read-only key for an object \( o \), \( r_k_o \), only if no other thread is holding a read-write key for \( o \), \( w_k_o \). In contrast, a thread can acquire \( w_k_o \) only if no other thread is holding \( w_k_o \) or \( r_k_o \). Any read from \( o \) without \( r_k_o \) or \( w_k_o \) and any write to \( o \) without \( w_k_o \) imply unordered memory access—the access can conflict with some other threads’ concurrent access on \( o \), resulting in a data race.

Example. Figure 1 depicts how key-enforced access works for exclusive write and read shared. Two threads, \( t_1 \) and \( t_2 \), access a shared object, \( o \), within their critical sections, \( s_a \) and \( s_b \), by obtaining two independent locks, \( l_a \) and \( l_b \), respectively (i.e., under ILU).

Figure 1a depicts an instance of exclusive write. In this example, \( t_1 \) executes first and acquires a read-write key for \( o \), \( w_k_o \) (line 2). Then, \( t_2 \) requests the read-only key, \( r_k_o \), but fails to acquire it because \( t_1 \) holds \( w_k_o \) (line 3). Hence, when \( t_2 \) attempts to read from \( o \), it results in an access violation (lines 5–6).

Algorithm 1: Key-enforced race detection algorithm.

- **t**: thread
- **s**: critical section
- **o**: sharable object
- **w_k_o**: read-write key for \( o \)
- **r_k_o**: read-only key for \( o \)
- **K(t)**: set of keys held by \( t \)
- **K_R(s)**: set of keys for \( s \) with read-only permissions
- **K_W(s)**: set of keys for \( s \) with read-write permissions
- **K_F**: set of keys no thread holds

```plaintext
while t is running do
  if t enters s then
    push(K(t))
    if (w_k_o \in K(t)) \text{ or } (r_k_o \notin K(t)) then
      log potential race
      return
    else if t is executing s then
      K(t) ← K(t) \cup \{r_k_o\}
      K_R ← K_R \cup \{r_k_o\}
      K_F ← K_F \setminus \{r_k_o\}
    if w_k_o \notin K_W(s) then
      K_R(s) ← K_R(s) \cup \{r_k_o\}
  else if t is executing s then
    K(t) ← K(t) \setminus \{w_k_o\}
    K_F ← K_F \setminus \{r_k_o\}
    K_W(s) ← K_W(s) \setminus \{w_k_o\}
    K_R(s) ← K_R(s) \setminus \{r_k_o\}
  if t writes to o and w_k_o \notin K(t) then
    if (w_k_o \notin K_F) \text{ or } (r_k_o \notin K_F \cup K_R) then
      log potential race
```

Figure 1b depicts an instance of shared read. Here, \( t_1 \) executes first but acquires \( r_k_o \) (line 2). Therefore, \( t_2 \) can successfully acquire \( r_k_o \) as well (line 3) and no violation is reported.
releases a key $k$, and updates $K_R(s)$ and $K_W(s)$ according to the keys acquired while executing $s$.

If a thread $t$ enters a critical section $s$, our algorithm first backs up its current $K(t)$ (lines 2–3). Then, $t$ is given a subset of $K_R(s)$ that no thread holds with read-write permission and a subset of $K_W(s)$ that no other threads currently hold (line 4). Furthermore, it updates $K_F$ to reflect that $t$ exclusively acquired some keys, while updating $K_G$ to show that the thread acquired some keys with read-only permissions (lines 5–6). Then, when $t$ exits $s$, our algorithm releases the keys that $t$ acquired either at the start of or during the execution of $s$ (lines 7–9).

If $t$ attempts to read from $o$ without $r_{k_o}$ or $w_{k_o}$ (line 10), our algorithm checks whether another thread holds $w_{k_o}$ (line 11). If some thread $t_o$ holds $w_{k_o}$, it implies that $t_o$ can write to $o$ any time before or after $t$ reads $o$. Therefore, this is a potential data race (line 12). If no thread holds $w_{k_o}$ and $t$ is executing a critical section $s$, it claims $r_{k_o}$ to prevent a concurrent write from another thread (lines 13–14). Furthermore, to track that $r_{k_o}$ is held by some thread, the algorithm includes the key to $K_R$ and removes it from $K_F$ (lines 15–16). Also, if $w_{k_o}$ is not in the scope of the critical section $s$, the algorithm includes $r_{k_o}$ into $K_R(s)$ (lines 17–18). On the other hand, if $t$ attempts to write to $o$ without $w_{k_o}$ (line 19), our algorithm checks whether any other thread $t_o$ holds $w_{k_o}$ or $r_{k_o}$ (line 20). If this holds, our algorithm treats the access as a potential data race (line 21). If the key is free and $t$ is executing a critical section $s$, the thread claims $w_{k_o}$ by adding it to $K(t)$ and $K_W(s)$ while removing it from $K_R(s)$, $K_R$, and $K_F$ (lines 22–26).

5 KARD DESIGN

5.1 Overview

We design KARD, a practical dynamic data race detector that realizes our key-enforced race detection algorithm (§4) with a commodity per-thread memory protection mechanism, MPK (§2.2). KARD leverages MPK’s per-thread read-only and read-write permissions on memory pages to protect sharable objects, accessed in critical sections, and to fulfill the requirements of key-enforced access.

Initially, KARD defines memory protection domains to classify sharable objects (i.e., heap and global variables) according to whether they are accessed in critical sections and whether those accesses were read or write (§5.2). To enable these domains, KARD implements (a) a consolidated unique page memory allocator to assign each sharable object unique virtual pages, allowing independent protection of each object using MPK and (b) an on-demand sharable object tracking scheme to accurately place objects in their respective domains (§5.3).

During program execution, KARD identifies new shared objects and enforces the protection domains for threads during critical section execution by carefully assigning protection keys to threads within distinct critical sections (§5.4).

Lastly, on access violations of protection domains, KARD performs automatic analysis to filter out redundant or non-racy violations, including initialization event detection, protection interleaving, and faulting address-based pruning (§5.5).

5.2 Memory Protection Domains

KARD classifies a program’s sharable objects into three domains: Read-only, Read-write, and Not-accessed. The domains are enforced with different protection keys to ensure different access semantics on each domain during execution.

Read-only domain. Each shared object that has been only read within critical sections belongs to the Read-only domain protected using $k_{ro}$ ($k_{14}$). In KARD, all threads (whether in critical or non-critical sections) have $k_{ro}$ with a read-only permission, so they can always read these objects. However, write access on it is prohibited for domain migration or data race detection (§5.5).

Read-write domain. Each shared object that has been written at least once within critical sections belongs to the Read-write domain, and is protected using one of 13 protection keys ($k_1$ to $k_{13}$). These protection keys are only provided to a thread that is executing a critical section, with either read-only or read-write permissions. To allow shared reads, multiple threads can obtain the same Read-write domain key with read-only permission. However, to ensure exclusive write, only a single thread can obtain a Read-write domain key with read-write permission at a time.

Not-accessed domain. Each newly created sharable object belongs to the Not-accessed domain, and if it is accessed within a critical section, it is migrated to either Read-only or Read-write domain. KARD protects new sharable objects using $k_{na}$ ($k_{15}$), and retracts $k_{na}$ from threads during their critical section execution. This allows KARD to determine if a thread accessed a newly created sharable object within its critical section via an access violation.

Finally, all memory regions must have a protection key when MPK is enabled. Therefore, KARD protects memory objects that are not sharable (e.g., thread-local variables) or should always be accessible to all threads (e.g., mutex variables) using the default key, $k_{def}$ ($k_0$ in current Intel CPUs).

5.3 Sharable Object Tracking

KARD tracks sharable objects to identify which ones are shared (i.e., read or written in critical sections) and changes their protection domains using MPK. However, this presents two challenges. First, MPK works at the granularity of pages (typically 4 KiB) but native allocators might create many objects in a single page. Second, accurately determining whether an object is shared and identifying the access type (i.e., read or write), without comprehensive memory access instrumentation, is non-trivial. To overcome these challenges, KARD implements consolidated unique page allocation and an automated shared object identification scheme.

Consolidated unique page allocation. Existing heap allocators store multiple objects in the same page to reduce memory consumption, which is incompatible with KARD’s protection. Since objects stored in the same page can belong to different protection domains, such compact allocation would result in extraneous access violations. This hampers both accuracy and performance of KARD.

To ensure per-object protection of heap objects, KARD replaces a program’s heap allocation routines (e.g., malloc() and new()) with its custom memory allocation routines that assign unique virtual pages to each object. In addition, KARD maintains the metadata (i.e.,
Automated shared object identification. Kard progressively identifies shared objects, from the list of all sharable objects, whenever critical sections execute. In particular, Kard traps every critical section execution with compiler instrumentation and prevents threads executing critical sections from accessing sharable objects not previously identified as shared. Hence, if the thread accesses such an object, a #GP will occur.

Kard traps critical section entries and exits by replacing synchronization calls, e.g., lock() and unlock(), with corresponding wrapper functions. Also, Kard provides the virtual address of a synchronization call site to the wrapper function to differentiate between critical sections during execution.

Figure 3a illustrates shared object identification during critical section execution. When a thread t1 enters a critical section, Kard revokes the access of t1 to k_m (a). Thus, a protection fault (#GP) related to k_m implies that t1 accessed a sharable object o_in the Not-accessed domain (b). Using the faulting address and access type (i.e., read or write) from the #GP, Kard migrates the object o_in to either the Read-only (i.e., k_reads) or Read-write (i.e., one of k1 to k13) domain according to the access type (c). Then, Kard updates an internal data structure, the section-object map (d), that tracks the shared objects accessed in each critical section and is used for domain enforcement. Lastly, t1 acquires the key protecting o_in if it did not hold the key before (e) (refer to §5.4).

Similarly, if a critical section raises a #GP because it attempts to write to an object belonging to the Read-only domain, Kard migrates the object to the Read-write domain.

5.4 Domain Enforcement

While progressively identifying shared objects (§5.3), in the same execution, Kard enforces protection domains during critical section executions to detect data races using key-enforced access (§4). Each identified shared object (§5.3) is assigned a protection key, and a thread either proactively (at a critical section entry) or reactively (during critical section execution) acquires the key. When a thread exits a critical section, it release the keys acquired within the critical section.
Effective key assignment. KARD uses several rules to smartly assign keys to identified shared objects. Ideally, each shared object (in the Read-write domain) should be assigned a unique key to enforce different access semantics for each critical section. However, due to MPK’s hardware limitation, KARD has a limited number of keys for objects migrated to the Read-write domain (i.e., 13).

KARD follows three rules to effectively use protection keys. First, if a faulting thread holds one or more protection keys, KARD assigns one of the held protection keys to the object (using pkey_mprotect()). Second, if the faulting thread does not hold any protection key (e.g., the first write access on a sharable object in a critical section), KARD looks for an unassigned protection key, protects the object with the key, and allows the thread to acquire the key.

Third, if all protection keys are assigned, KARD either (a) recycles an assigned key that no thread is currently holding or (b) shares a key between threads if all keys are currently held. Note that recycling is preferable since KARD can move the objects that have been protected by the recycled key to the Read-only domain. This allows KARD to trap potential data races (through writes) on the recycled objects. Thus, recycling neither harms KARD’s accuracy nor preciseness, but only slows down the program due to repeated domain migration. In contrast, sharing can result in false negatives (refer to §7.3). Nevertheless, our evaluation shows that both recycling and sharing is rare (§7.3); hence, in practice, their impact is minor.

Proactive key acquisition. With KARD, a thread will proactively acquire keys, belonging to already identified objects, when it enters a critical section. In particular, protection keys are acquired at critical section entries using a user-level instruction, WRPRKU. Note that key acquisition can be racy; thus, KARD employs internal synchronization (i.e., atomic operations), like general lock functions, to prevent such problems.

Figure 3b illustrates how a thread acquires keys at a critical section entry. When a thread enters a critical section, KARD looks up the section-object map to find the shared objects accessible in the critical section and associated keys (1). Then, KARD checks the key-section map, a data structure that maintains which sections (and threads) currently hold what keys, to determine which keys are available (2). The thread can acquire an available key with (a) read-write permission if no other thread holds the key or (b) read-only permission if no other thread holds the key with read-write permission. In the figure, a thread t1 acquires k1 with read-write permission, but fails to acquire k2 because another thread t2 is holding it (3). Lastly, KARD pushes the thread’s current keys in a thread-local stack to restore when it exits the critical section.

Reactive key acquisition. At some object identifications (§5.3), a thread must reactively acquire a key assigned to a newly identified shared object, if the thread did not acquire that key at critical section entry. This reactive key assignment is performed by KARD’s fault handler (explained in §5.5). The fault handler, however, cannot use WRPRKU for this key assignment because the program thread is not currently running. Instead, the fault handler modifies the thread’s stored process context for the PRKU register [43, 57] to allow the thread to possess the key when it is scheduled again.

Key release. When a thread exits a critical section, the thread releases protection keys acquired reactively or proactively (Figure 3b-3). More specifically, if a thread exits to a non-critical section, it releases all of its protection keys (k1 to k13, except k_{old}) and acquires k_{new}. On the other hand, if the thread exits a nested critical section (i.e., it is still within a parent critical section), it reverts back to its old keys from the thread-local stack. Lastly, KARD timestamps (using RDTSACP) each time a thread releases protection keys to consider a fault handling delay during data race analysis (refer to §5.5).

5.5 Race Detection and Filtration
KARD redirects all protection faults (#GPs) to its custom fault handler to detect potential data races while handling missing or spurious violations due to fault handling delay and initialization events. Furthermore, KARD employs a protection-interleaving scheme to effectively filter out false positives. Lastly, KARD automatically prunes redundant violations.

Protection fault (#GP) redirection. KARD registers a custom fault handler to trap all MPK-based #GPs and obtain information related to the faulting address, including protection key, access type, and process context (e.g., instruction pointer).

The system raises a #GP for attempted access on (a) sharable object belonging to the Not-accessed domain (protected by k_{old}), (b) shared object protected with a key that the thread did not acquire, or (c) shared object protected with a key that the thread acquired with read-only permissions. Considering (a), KARD assigns a protection key to the object (refer to §5.4). The remaining scenarios, (b) and (c), could be data races but require further analysis to check whether the faulted key is held by another thread with read-write permissions.

Figure 3c illustrates a potential data race scenario. In this example, we assume that t2 executes first and acquires a protection key, wk2, to write in an object o2. Then, when t1 executes, it fails to acquire a key rk2 because t2 is holding wk2, according to the key-section map (1). Hence, when t1 tries to read o2, it raises a fault (2). KARD checks whether the key protecting o2 is currently held by any thread (3), and confirms there is a data race between t1 and t2.

Note that KARD uses timestamps to assess whether a protection key was held when the #GP occurred because the key might be released by the time the handler is invoked. KARD checks whether the time difference between key release and fault handler invocation is below the average fault handling delay (e.g., 24,000 cycles on our machine whose specifications are described in §7.1).

Protection interleaving. With KARD, a thread proactively acquires keys at critical section entries and a single key protects the entire object to minimize runtime overhead and efficiently use a limited number of protection keys, respectively. This, however, potentially introduces false positives due to (a) conditional branches in critical sections and (b) concurrent access to different offsets in an object (detailed analysis in §7.3).

KARD mitigates false positives using a protection-interleaving scheme that alternates protection keys assigned to faulted objects to further test the accuracy of a raised protection fault. Figure 4 illustrates protection interleaving between two threads t1 and t2. In particular, t2 raises a #GP for an object o that is protected by a key k1, held by t1 (line 6). KARD forcefully protects o with one of the keys held by t2 (or protects o with a free key and assigns the key to t2), k2, and allows t2 to proceed (line 7). Later, if t1 accesses o, it will raise another #GP (line 8). Thus, KARD observes
Automated pruning. KARD automatically prunes redundant and non-racy violations using its metadata (e.g., section-object map). It prunes (a) redundant faults of the same object at the same offset from different threads and (b) spurious faults due to access at different offsets of the same object (captured by protection interleaving).

Potential data race record. Based on the filtered #GP and metadata, KARD constructs potential data race information including: (a) both sections that raise the fault and holds the key, (b) the faulted object, (c) the faulting thread’s access type, (d) thread identifiers and process contexts, and (e) timestamp.

6 IMPLEMENTATION

We implemented KARD using the LLVM 7 compiler suite [32]. Our implementation consists of backend LLVM function and module passes, as well as a runtime library. The runtime library has three main components: (a) a custom allocator along with wrapper functions for standard heap allocation, (b) wrapper functions for POSIX, Pigg [5], and NGINX [41] synchronization functions, and (c) a fault handler. Our backend code consists of 966 Lines of Code (LoC) and the runtime library consists of 1,888 LoC written in C/C++, counted using sloccount [2].

For simple management, KARD’s custom allocator uses standard C++ data structure libraries to manage allocated memory objects and returns a multiple of 32 B to each memory allocation request. Currently, KARD invokes mmap() for each memory allocation, so it can suffer from high performance overhead if an application frequently allocates memory objects. However, such applications are rare (refer to §7.2). In the future, to reduce the overhead of frequent mmap() calls, KARD can recycle de-allocated virtual pages [64]. Moreover, KARD does not consolidate page-aligned global variables, thereby increasing the overall memory consumption of the system. We confirm that this does not affect the runtime performance of our tests, and KARD’s reported memory overhead is over-estimated rather than under-estimated.

KARD does not currently cover non-locking synchronization primitives including ad-hoc ones. Generally, ad-hoc synchronization primitives are considered harmful [59]. If such synchronization must be employed, KARD’s backend can be updated either using annotations or static analysis [59] to trap their execution and enforce memory protection.

7 EVALUATION

This section evaluates KARD in terms of performance overhead, effectiveness, scalability, and memory consumption.

7.1 Experimental Setup

We conducted all experiments on a Dell Precision 7820 Workstation featuring two Intel Xeon Silver 4110 processors where each processor consists of 16 logical cores at 2.1 GHz (32 logical cores in total), and 32 GiB of memory. The workstation runs Ubuntu 18.04.2 LTS whose kernel version was 4.15.

7.2 Performance

This section illustrates KARD’s performance overhead while executing a diverse set of benchmark and real-world applications. In general, there are three major factors affecting KARD’s performance: (a) the number of protected sharable objects, (b) the number of critical section entries, and (c) data TLB (dTLB) miss rate. First, the number of pkey_mprotect() system call invocations linearly depends on the number of sharable objects (invoked at object allocation and migration). Second, KARD traverses and updates the section-object and key-section maps to change the protection keys assigned to threads whenever they enter critical sections. Lastly, since KARD’s memory allocator assigns each sharable object unique virtual page(s), it consumes more virtual address space, hence, programs can suffer additional dTLB misses.

Settings and notation. We compare KARD’s performance against (a) applications without data race detection (referred to as Baseline), (b) applications using KARD’s memory allocator but no race detection (referred to as Alloc), and (c) applications with TSan (referred to as TSan). Alloc implements the impact of KARD’s memory allocator on its overall performance. For Baseline and TSan, the applications were built using unmodified clang-7. We used the same compiler flags (except for race detection flags) for all four cases.

We ran most of the experiments using 4 threads. Despite being a modest configuration for production, 4 threads are suitable for testing, which is KARD’s main focus. During testing, the developer controls the number of program threads and generally tries to simplify the testing scenario to optimize resource usage and simplify failure diagnosis. Note that a well-known data race study [36] shows...
that even 2 threads can manifest more than 95% of data race bugs; hence, 4 threads are appropriate for most data race testing scenarios.

**Benchmarking suites: PARSEC and SPLASH-2x.** We evaluated Kard with the PARSEC/SPLASH-2x benchmark version 3.0-beta-20150206 [8]. We ran all benchmarking applications that use locks and do not require code-rewriting to build using clang-7. We decided to omit benchmarks that do not use locks because they have no overhead under Kard and that require code rewriting because it can affect the benchmark’s intended behavior.

Results. Table 3 shows that Kard incurs a low performance overhead with a geometric mean, compared to Baseline, of only 7.0%. Most of the benchmark applications incurred a very low overhead except a few that frequently enter critical sections or have many protected sharable objects. Especially, the two benchmarking tests, fluidanimate and ocean_cp, that entered critical sections around 4.4 million and 1.8 million times within 3.3 s, respectively, incurred a higher overhead than the average. We conjecture that such behavior is more congenial to benchmark tests, and we did not observe this in our real-world applications (e.g., NGINX entered critical sections only around 200,000 times within 15.2 s in our evaluation). Besides, despite fewer critical section entries, water_nsquared has many protected shared objects; hence, it suffered from a high dTLB pressure and showed a high performance overhead.

Interestingly, applications with few sharable objects (e.g., lu_cb and ocean_cp) ran slightly faster with Kard, compared to Baseline. The reason is that Kard’s memory allocator trades off simplicity for memory consumption ($\S$7.5) and, therefore, we observe the same trend with Alloc. Importantly, even if we compare Kard’s performance on each benchmarking application against the best performance of either Baseline or Alloc, the overall geometric mean of Kard’s performance overhead only rises to 8.7% from 7.0%.

Lastly, Kard executed approximately two orders of magnitude faster than TSan, under 4 threads, because Kard does not employ expensive compiler instrumentation of memory accesses. Nevertheless, TSan covers more diverse data race types than Kard (refer to Table 2).

**Real-world applications.** We evaluated Kard with four real-world applications: web server (NGINX 1.17.1 [41]), key-value store (memcached 1.5.16 [17]), compression software (pigz 2.2.4 [5]), and download manager (Aget 0.4.1 [19]). The geometric mean of Kard’s overhead, under 4 threads, was 5.3% for these applications, compared to Baseline.

**Web server—NGINX.** Web servers employ multi-threading to serve multiple clients simultaneously with low latency. We used ApacheBench (ab) [56] to send 100,000 requests through 100 concurrent clients to an NGINX web server. We ran four different tests to retrieve files of sizes of 128 kB, 256 kB, 512 kB, and 1 MB, from the NGINX web server. We chose the file sizes after consulting existing web server traffic reports [5]. The average latency overhead across the tests was 15.1%. In particular, we observed that the overhead was higher when the file size is smaller. For example, the ab tests for 128 kB file showed an overhead of 58.7% while the overhead for the 1 MB file was 8.8%. Thus, the additional I/O overhead of larger files amortized Kard’s runtime overhead.

**Key-value store—memcached.** Concurrency is a large enabling of modern key-value stores. We evaluated Kard against memcached [17], a popular key-value store, using a benchmarking tool, twemperf [47]. We configured twemperf to send 20,000 set requests of 1 B size through 2,000 concurrent connections. The overhead
was negligible. In particular, memcached accessed very few shared objects in its critical sections and had a modest number of critical section entries; therefore, the overhead remained low, despite a few key sharing and recycling events (refer to §7.3).

Other applications—Aget and pigz. Aget [19] accelerates file download using multiple threads. We used Aget to download a Linux kernel image (105 MB size). To account for network delays, we downloaded the file 100 times. Kard’s slowdown was only 1.4%.

Another application, pigz [5], compresses or decompresses files using multiple threads. Our test comprised of decompresing the Linux kernel image (105 MB) 100 times using 4 concurrent threads. Kard’s average overhead was 5.1%.

### 7.3 Effectiveness

This section analyzes Kard’s effectiveness and presents results related to real-world data races reported by Kard.

**Theoretical analysis.** Table 4 provides an overview of the potential issues that Kard might face and various mitigation strategies adopted by Kard, in response.

<table>
<thead>
<tr>
<th>Potential issue</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>False negative</td>
<td></td>
</tr>
<tr>
<td>Sharing protection keys</td>
<td>Share keys amongst disjoint sections</td>
</tr>
<tr>
<td>False positive</td>
<td></td>
</tr>
<tr>
<td>Different offset in an object</td>
<td>Employ protection interleaving</td>
</tr>
<tr>
<td>Non-access in critical section</td>
<td>Employ protection interleaving</td>
</tr>
</tbody>
</table>

### Table 4: Potential false negative and positive scenarios for Kard, and how Kard mitigates them.

<table>
<thead>
<tr>
<th>Number of memcached threads versus the unique and concurrent critical sections (CS), recycling events, and sharing events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of threads</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Total executed CS</td>
</tr>
<tr>
<td>Uniquely executed CS</td>
</tr>
<tr>
<td>Maximum concurrent CS</td>
</tr>
<tr>
<td>Key recycling events</td>
</tr>
<tr>
<td>Key sharing events</td>
</tr>
</tbody>
</table>

Key sharing case study. To confirm whether false negatives due to key sharing can be a problem in practice, we ran all our benchmark and real-world applications with up to 32 threads (the maximum number of hardware threads our system supports §7.1). We found that only 1 out of 19 applications, memcached, required key sharing, but its sharing events were extremely rare: less than 0.07% of total executed critical sections.

In particular, memcached has 121 critical sections, based on our source code analysis, and executes many of them concurrently; hence, Kard had to employ key sharing. Table 5 shows the total number of critical sections executed, how many of the executed critical sections were unique or concurrent at one time, and corresponding sharing and recycling events, while increasing the number of threads.

Despite executing 13–16 concurrent critical sections, memcached required key sharing very few times, 11–116 (only 0.007%–0.07% of the total executed critical sections). While increasing the number of threads increases the active critical sections and produces more key sharing events, the difference is minimal. This shows that even for complex real-world applications with many critical sections and executing many threads, such as memcached, few critical sections execute concurrently; therefore, the limited number of keys provided by MPK should be sufficient in most cases.

We also observed a few key recycling events, 724–808 times (only 0.44%–0.49% of total executed critical sections). Note that recycling does not impair Kard’s accuracy or preciseness (refer to §5.4).

We assume that a developer will use configurations that minimize key sharing events (i.e., a small number of threads) to avoid potential false negatives (Table 4). Even when configurations with high key sharing events (e.g., memcached with 32 threads) are employed, Kard can still probabilistically report a data race if it is triggered multiple times with different key sharing instances due to thread scheduling. Nevertheless, new hardware proposals or software fallback can avoid key sharing (refer to §8).

Real-world data races reported. Kard reported all real-world data race bugs that were also reported by TSan involving ILU with only 1 false positive (Table 6). Both Kard and TSan are schedule-sensitive; therefore, they might not produce the same number of data races on each run. However, we did not observe a variance for these applications.

Aget. Kard reported a single data race warning from Aget, similar to TSan. In particular, Aget writes to a single global variable (to
We observed that the main thread only updates the timing information. In particular, the heap variables were updated by a worker thread within its critical section and read by the main thread (outside its critical section). As for the global variable, its timing contents are updated by the main thread using a callback mechanism and read by another thread, within a critical section. We believe that this data race might be intentional since the main thread only updates the timing information.

NGINX. Both KARD and TSan reported a data race that originates from a race heap access in a critical section during NGINX’s initialization. This was the only data race warned by either of the tools, while executing NGINX.

pigh. KARD reported 1 false positive due to concurrent access at different offsets in a heap variable from pigh. Despite protection interleaving, KARD failed to prune this warning out because the corresponding critical section is too small such that KARD did not observe accesses from other threads. Therefore, it included the data race in the final report. Nevertheless, protection interleaving filtered out pigh’s other access violations within relatively large critical sections.

7.4 Scalability
KARD maintains its performance efficiency for most of the benchmarking applications even with up to 32 threads. Figure 5 shows the scalability of KARD while executing PARSEC and SPLASH-2x applications. The geometric mean of KARD’s performance overhead with 8, 16, and 32 threads, is 24.4%, 63.1%, and 107.2%, respectively. We observed that KARD scaled well for most benchmarks, except the three applications, fluidanimate, water_nsquared, and barnes, due to their large numbers of critical section entries and sharable objects. However, excluding such worst-case applications, the geometric mean of KARD’s overhead was only 5.8%, 12.4%, and 19.0%, for 8, 16, and 32 threads, respectively.

7.5 Memory Consumption
KARD incurs memory overhead due to (a) unique page memory allocation and (b) internal metadata like the section-object and key-section maps. First, despite page consolidation, KARD can waste memory if the allocated object size is not a factor of the fixed virtual page consolidation size (currently set to 32 B). Also, KARD does not currently consolidate the unique virtual pages of global objects (refer to §6); hence, it pays an additional memory cost that can be reduced in future implementations. Second, KARD consumes memory to maintain internal metadata, depending on the number of critical sections, sharable objects, and protection keys. Such memory consumption can be reduced by implementing optimized data structures for KARD instead of using standard C++ data structure libraries.

Despite the limitations of KARD’s implementation, considering the evaluated applications, KARD’s memory overhead is modest: a geometric mean of 68.0% for the benchmarking applications and 85.6% across our real-world applications, according to the Resident Set Size (RSS) [51] (Table 3). In particular, 10 out of 15 benchmarking applications have a memory overhead less than 10%. We observe that water_nsquared has the highest memory overhead. Upon closer inspection, we found that it allocates 128,000 of 24 B heap objects, making the unique page allocator waste memory (i.e., 8 B per-object since KARD allocates objects in multiples of 32 B). In contrast, although NGINX allocates many objects, its memory overhead is smaller than that of water_nsquared because the size of its objects is usually 32 B or 4 KiB. Thus, KARD can decrease the memory overhead by profiling the most common allocation size of a target program and using that size for allocation.

8 DISCUSSION
This section describes a potential problem that could occur with progressive shared object identification. Then, it presents ways to preserve KARD’s accuracy even in key sharing scenarios using software and advanced hardware memory protection implementations. Lastly, the section discusses possible KARD extensions that would allow KARD to detect non-ILU data races and data races on program binaries without requiring source code instrumentation.

Progressive identification. Progressive shared object identification and domain enforcement (refer to §5.3) can potentially open a tiny time window that allows a thread outside of its critical section to access a shared object being identified within a different thread’s critical section. KARD will not report such data races due to a lack of domain protection for the newly-identified shared object. However, we believe that such scenarios are extremely rare because the time window is so small and we did not observe them during the evaluation (refer to §7.3). Furthermore, KARD will report the data
race missed during identification if it occurs again during the same program execution. We leave such investigation to future work.

Software fallback and advanced hardware. Kard can overcome the limitations of MPK’s current implementation using software per-thread memory protection mechanisms, such as those employed by iThreads [7], or advanced hardware implementations of per-thread memory protection. Since MPK provides only 16 protection keys, Kard must share protection keys in rare occasions (refer to §7.5). However, Kard’s race detection algorithm is agnostic to the underlying memory protection mechanism, so it can revert to a software memory protection scheme [3, 10, 46] when it exhausts hardware protection keys. Nevertheless, software memory protection requires systems software changes and incurs significant performance costs (up to 100% [46]). In the future, Kard can be implemented on advanced hardware [50, 60] that allows up to 1000 protection keys to completely negate protection key limit issues.

Non-ILU extension. Kard can extend its race detection algorithm (refer to algorithm 1) to track data races that occur outside ILU’s scope, by updating the algorithm to acquire protection keys for shared variables outside critical sections. However, on current MPK hardware, such an extension would not be effective because the limited protection keys would result in many instances of protection key sharing (which can result in false negatives). Nevertheless, software fallback and advanced hardware can circumvent protection key limitations (as explained before) to make such extension feasible in the future.

Program binary extension. Kard can act directly on unmodified program binaries by intercepting standard library calls for heap memory allocation and thread management, and using a custom loader to handle global variables. For example, Kard can intercept library calls via LD_PRELOAD to use its memory allocator and update per-thread protection domains while differentiating synchronization call sites using return addresses. Furthermore, for position independent binaries (compiled with -fPIC), Kard can change the locations of global variables to store them in unique virtual pages. We leave such implementation to future work.

9 RELATED WORK
This section provides an overview of data race detection schemes that are related to Kard. It initially describes schemes that implement dynamic data race detectors using software or hardware memory protection or use other commodity hardware features like transactional memory and processor monitoring units. The section concludes by providing a comparison between dynamic data race detectors like Kard and static data race detection techniques.

Memory protection for data race detection. Several prior studies use software memory protection to detect data races. Multirace [45] uses minipages along with pointer swizzling to ensure per-thread view on a memory page, but requires expensive indirect memory access. ISOLATOR [46] and Abadi et al. [3] use a copy-on-write trick to ensure thread isolation. Whenever a thread writes a value into a shared read-only page, it will obtain a new private page copied from the original one. However, if the diverged pages have conflicting values, it is difficult to merge them to create a single view. Other schemes implement per-thread address spaces [10, 27, 35, 42] using kernel modifications. Such schemes invoke system calls and flush TLB entries to change per-thread permissions. Thus, they incur substantial performance overhead unlike Kard.

Virtual machine monitors have also been used to enable software memory protection for data race detection. In particular, SKI [23] uses a modified QEMU to analyze memory accesses at the virtual machine-level while ensuring schedule diversity. This allows SKI to detect data races and other kernel concurrency bugs without modifying the tested system. Unlike SKI, Kard uses efficient hardware protection mechanisms and selectively analyzes memory accesses to ensure very low impact on application performance.

Like Kard, Push [64] uses MPK’s efficient hardware memory protection to detect data races. However, Kard has three main technical contributions over Push. First, Kard proposes a key-based race detection algorithm that reports ILU data races using protection keys. Unlike Push’s design, which assumes complete knowledge of object sharing patterns through manual annotations, Kard’s algorithm is built for progressive identification of sharing patterns, which allows automated data race detection. Second, Kard implements efficient shared object identification, which is more than an order of magnitude faster than prior implemented identification strategies like Eraser’s [49]. In contrast, Push relies on extensive manual effort, such as 35 hours to annotate and modify the streamcluster application, highly undesirable in testing settings [34]. Lastly, Kard implements protection interleaving to mitigate false positives and precisely identify the actual byte offsets accessed by conflicting threads. In contrast, to detect sub-object data races, Push page-aligns each structure member and array element, resulting in potential compatibility issues with external libraries [40] and substantial memory overhead.

Other hardware approaches. TxRace [62] uses Transactional Synchronization Extensions (TSX) to reduce the overhead of TSan. However, TXS suffers from false positives because any interrupt or cache line eviction can affect its behavior and its monitoring capacity depends on the cache size [33, 54]. REPT [15] uses Intel Processor Trace and crash dump to realize reverse debugging. However, REPT cannot detect transient data race bugs that do not produce a crash.

Static data race analysis. Static detectors [11, 31] can detect some data races during program compilation with no performance overhead. A major limitation of such approaches is that they can potentially report many false positives that developers want to avoid [34]. In particular, static techniques rely on imprecise pointer analysis [30, 55] that fails to accurately resolve function pointers [4] and cannot match data accesses to dynamically-allocated objects (e.g., heap-based). In contrast, dynamic detectors, including Kard, do not suffer from such problems, so they report fewer false positive data races than static analysis techniques.

10 CONCLUSION
Kard is a dynamic data race detector with a very low performance overhead of 7.0% with PARSEC and SPLASH-2x, and 5.3% with real-world applications, under the common testing scenario of 4 threads. Kard uses per-thread memory protection from Intel MPK to detect all data races involving inconsistent lock usages with a
We thank our shepherd, Brandon Lucia, and the anonymous reviewers for their valuable comments and suggestions. This work was partly supported by an Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.2020-0-01840, Analysis on technique of accessing hardware limitations of MPK to have a low false positive rate and key-enforced race detection algorithm. KARO overcomes various hardware limitations of MPK to have a low false positive rate and a modest memory overhead.

ACKNOWLEDGMENTS

We thank our shepherd, Brandon Lucia, and the anonymous reviewers for their valuable comments and suggestions. This work was partly supported by an Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.2020-0-01840, Analysis on technique of accessing hardware limitations of MPK to have a low false positive rate and key-enforced race detection algorithm. KARO overcomes various hardware limitations of MPK to have a low false positive rate and a modest memory overhead.

REFERENCES


