Abstract
OS design is traditionally heavily intertwined with protection mechanisms. OSes statically commit to one or a combination of (1) hardware isolation, (2) runtime checking, and (3) software verification early at design time. Changes after deployment require major refactoring; as such, they are rare and costly. In this paper, we argue that this strategy is at odds with recent hardware and software trends: protections break (Meltdown), hardware becomes heterogeneous (Memory Protection Keys, CHERI), and multiple mechanisms can now be used for the same task (software hardening, verification, HW isolation, etc). In short, the choice of isolation strategy and primitives should be postponed to deployment time.

We present FlexOS, a novel, modular OS design whose compartmentalization and protection profile can seamlessly be tailored towards a specific application or use-case at build time. FlexOS offers a language to describe components’ security needs/behavior, and to automatically derive from it a compartmentalization strategy. We implement an early prototype of FlexOS that can automatically generate a large array of different OSes implementing different security strategies.

CCS Concepts
• Software and its engineering → Operating systems; • Security and privacy → Operating systems security.

1 Introduction
To create secure and fast software, programmers can use three main approaches offering various trade-offs between human effort, safety guarantees and runtime performance: software verification, runtime checking and hardware isolation. Today’s software statically commits to one or a combination of these approaches. At design time, systems are built around the protection ensuing from these mechanisms; changing them after deployment is rare and costly.

In operating systems, the current landscape (illustrated on Figure 1) broadly consists of micro-kernels [24, 29], which favor hardware protection and verification over performance, monolithic kernels [8], which choose privilege separation and address spaces to isolate apps, but assume all kernel code is trusted, and single-address-space OSes (SASOSes), which attempt to bring isolation within the address space [10, 23, 32], or dump all protection for maximum performance [30, 36, 43].

OS implementations are heavily interlinked with the protection mechanisms they rely upon, making changes to them difficult to implement. For instance, removing user/kernel separation [37] requires a lot of engineering effort, as does breaking down a process into multiple address spaces for isolation purposes [27]. This is the case despite the fact that alternative approaches can be used to provide the same guarantees. First, verification and software hardening (SH) such as SFI can help ensure memory isolation between separate components even if they run in the same address space, thus avoiding the need for hardware isolation [19, 52]. Second, hardware isolation, SH and runtime property checking can be used to check that certain correctness properties hold (e.g. when specified as pre and post conditions), thus relieving the user from needing to prove code correctness statically against a specification [47]. Third, both software verification and protection domains can be used to ensure (a form of) control-flow integrity between components, guaranteeing...
that code execution starts only at well-defined entry points, without needing software runtime checks [53].

The rigid use of safety primitives in modern OSes poses a number of problems. First, when the protection offered by hardware primitives breaks down (e.g. Meltdown), it is difficult to decide how they should be replaced, and with what costs. In cases where multiple mechanisms can be used for the same task (e.g. SH and verification), choosing the primitive that provides the best performance depends on many factors such as the hardware, the workload, etc., and should ideally be postponed to deployment time, not design time. Locking the design to a certain isolation primitive will result in poor performance in many scenarios.

Second, computer hardware is becoming heterogeneous [54] and certain primitives are hardware-dependent (e.g. Intel Memory Protection Keys – MPK [12]). When running the same software on different hardware, how can we minimize the porting effort while preserving safety?

Software modularization should, in principle, provide better robustness and security. Most software, including OSes, integrates modules from different sources, with various levels of trust. Unfortunately, the isolation primitives assumed by the module designers affect the way in which a module can be used, limiting its usefulness. Take, for instance, a formally verified OS subsystem: how does one go about embedding it into a larger project while still maintaining its safety properties? Clearly, if one embeds this component alongside untrusted C code, its verified properties may not hold in practice.

This leads us to the following research problem: How can we enable users to easily and safely switch between different isolation and protection primitives at deployment time, avoiding the lock-in that characterizes the status-quo?

Our answer is FlexOS, a novel, modular OS design whose compartmentalization and protection profile can easily and cost-efficiently be tailored towards a specific application or use-case at build time, as opposed to design time as it is the case today. To that aim, we extend the Library OS model (LibOS) and augment its capacity to be specialized towards a given use case, historically done for performance [18, 26], towards the security dimension.

With FlexOS, the user can decide at build time which of the fine-grained OS components should be compartmentalized, as well as how to instantiate isolation and protection primitives for each compartment. FlexOS allows developers to easily explore the trade-offs than can be achieved with different isolation technologies and granularities, and to select the best security/performance profile for their use case. Concretely, our research contributions are:

- The design and implementation of FlexOS, a novel framework for effortlessly investigating performance vs. security trade-offs in operating systems.
- The identification of fundamental primitives that are needed in order to provide isolation and protection via a wide range of software and hardware-based mechanisms.
- A preliminary evaluation showing how FlexOS can be used to explore a wide array of security/performance profiles for two apps: iperf and Redis.

2 Design Overview

The goal of FlexOS is to allow developers and OS researchers to easily inspect and select different points in the security vs. performance trade-off space. Exploring such a space is far from trivial, and our aim is also to automate such exploration. Here, various strategies could be followed:

- Given a performance target and a set of predefined compartments (e.g. isolate the application and the network stack from everything else), find the combination of isolation primitives that maximizes security within a certain performance budget.
- Given a set of safety requirements (e.g. no buffer overflows), find a compliant instantiation that yields the best performance or that can run on the largest number of devices (based on the availability of hardware-based mechanisms).

Both objectives above have in common the need to describe the security attained by each mechanism, and the implications of running one software component in the same compartment as another one.

We base our design as an extension of the LibOS model [18], since LibOSes are by nature divided into fine-grained components/libraries. Our approach consists in supporting a set of hardware and software hardening mechanisms, and complementing the API of each such library with FlexOS metadata specifying 1) the expected memory access behavior of other components running in the same compartment as the library for its safety properties to hold; 2) the areas of memory this library can access in normal but also adversarial operation (for example if the library’s execution flow is hijacked); and 3) API specific information.

Such metadata are created manually for each library by its developer, a one-time and relatively low effort for the library’s author. The metadata purpose is to capture the effects upon the overall safety properties of running this library alongside other libraries in the same or in a different compartment.
For instance, here is an example describing FlexOS’ formally verified scheduler that we have implemented in Dafny [31]:

```plaintext
[Memory access] Read(Own,Shared); Write(Own,Shared)
[Call] alloc::malloc, alloc::free
[API] thread_add ( . . . ); thread_rm( . . . ); yield( . . . )
[Requires] *(Read,Own), *(Write,Shared), *(Call, thread_add), * . . .
```

The description concisely specifies that (1) the library accesses its own memory and a segment shared with other libraries (e.g., its callers), that (2) it only uses functions provided by the memory allocator, (3) which functions it exposes as its API, and that (4) it expects other libraries to be able to read its own memory (but not write to it) and be able to write in shared memory.

Consider now a component written in an unsafe language, such as C, that is deemed potentially unsafe (perhaps due to variable-length writes to a buffer that cannot be proven safe statically); its description will read:

```plaintext
[Memory access] Read(); Write()
[Call] *
```

This specification simply outlines that the control/data flow of this component may be hijacked at runtime, resulting in arbitrary code execution/memory access. Since there is no Requires clause, this means other libraries should not be prevented from writing to memory owned by this library.

Given two libraries and their metadata, we now have enough information to automatically decide whether they can run in the same compartment. If both libraries have no Requires clause, the answer is yes. If any of the libraries has such clauses, each clause can be automatically checked in the presence of the other library. In our example above, for its verified properties to hold, the scheduler expects others to only read, not write, to its own memory. The C component, on the other hand, could write to all memory it has access to (in its compartment) - thus breaking the expectation: as a result, these two libraries cannot be run in the same compartment.

Armed with information about pair-wise incompatibility, selecting the smallest number of compartments in a FlexOS image can be reduced to the classical graph coloring problem: each library is a vertex, and an edge connects two incompatible libraries. Graph coloring assigns the smallest number of colors to the vertices of a graph such that no two adjacent vertices have the same color. For each color, we will have two versions now, one with SH and one without. SH techniques are handled similarly. To enumerate feasible deployments with SH, we proceed as follows: 1) for each library that writes to all memory, enable DFI / ASAN; 2) for each library that can execute arbitrary code, enable CFI.

The result of this step will be a list of libraries that have two versions: one with SH, and one without. We then iterate through all combinations of such library versions and run the graph coloring algorithm described above. This will result in as many colorings as there are possible combinations of libraries. Consider our example above: the unsafe C library will have two versions now, one with SH and one without SH. When put together with the scheduler in the same image, the SH version will be able to share a compartment with the scheduler, while the original version will require a separate compartment.

**Handling pre and post conditions.** The approach we took to handling memory access requirements could also be applied to pre-conditions that certain API functions may request to be true when called. For instance, in the case of the scheduler, one of thread_add’s preconditions is to not add a thread that has already been added. In such cases, FlexOS could be extended to automatically check whether the pre-conditions always hold on call (based on a static analysis of the call graph); if they don’t, runtime checks should be added to ensure they do hold. In our current prototype, we add these checks manually in our scheduler code; in future work we intend to explore ways of deriving this automatically.

**FlexOS Architecture.** FlexOS is based on a modular LibOS (Unikraft, a unikernel framework [30]) and allows fine-grained OS software modules to be placed in compartments (see Figure 2). Note that the granularity of such modules is much more fine-grained than that of traditional microkernel/multi-server OSes. Components in FlexOS are separated via gates which are made up of the API each compartment exposes. The gates also implement isolation between compartments, and
can leverage different isolation mechanisms depending on the available hardware (e.g. protection keys [12, 14], capabilities [55]) or software (e.g. CFI or ASAN).

Gates are instantiated at link time based on the requirements provided by the user or automated tools. Implementations vary from cheap function calls all the way to expensive RPC across VM boundaries. Depending on the chosen gates, the compartments will be running in the same protection domain or in different ones. Further, each compartment can be individually hardened by using SH without code changes.

FlexOS leverages Unikraft’s micro-library granularity (e.g. a scheduler, a memory allocator or a message queue are all micro-libs) but replaces each micro-lib’s standard function-call based API with call gates. In the porting process, developers replace cross-micro-libs function calls with gate placeholders. Once replaced by a particular implementation in the linking stage, gates take care of executing the function call in the foreign compartment, and of copying the return value back. Programmers do not need knowledge of the internal functioning of gates; all gates are exposed by the same, simple API:

```c
rc = listen(sockfd, 5); // before porting
uk_gate_r(rc, listen, sockfd, 5); // after porting
```

Programmers also annotate data shared with other micro-libs so that they are allocated in shared areas according to the compartmentalization graph.

FlexOS’s build system extends Unikraft’s to allow specifying how many compartments the resulting image should have, how they should be isolated, and whether SH techniques should be applied to one or multiple of these. Using this information, FlexOS’s builder will generate the required protection domains (one per compartment) and replace the call gate placeholders with the relevant code. For libraries in the same compartment, it will replace the call gates with direct function calls. For inter-compartment crossings, it will use the appropriate gate for switching protection domains: in our example in Figure 2, we have three separate compartments.

Using these basic primitives, a developer will be able to easily experiment with various isolation techniques to find the fastest implementation for a given task. We show, via experiments in §4, how we can create several networking images that do not trust the networking stack, with vastly different performance and security characteristics.

### 3 Implementation Prototype

To demonstrate its practicality, we implement a prototype of FlexOS on top of Unikraft v0.4 [49] in 1.5K LoC. Gate support is provided by two isolation mechanisms, referred to as isolation backends: Intel MPK and VM (EPT) isolation. SH support is available with CFI, ASAN, etc. We ported a subset of the Unikraft micro-libraries to FlexOS, manually created compartment specifications and identified shared data to showcase the trade-offs FlexOS enables; implementing the automated approach to defining compartments is left as future work. Note that although we focused on virtualized environments for this prototype, nothing fundamentally precludes FlexOS to run as a bare-metal OS.

**Intel MPK Backend.** Intel MPK is a mechanism providing low-overhead intra-address space memory isolation [1, 5, 46] at the granularity of a page. Our MPK backend places each compartment in its own MPK memory region, including static memory, heap, stack, and TLS. MPK permissions for the thread executing on a core are held in a register named PKRU. Since any compartment can modify its value, the MPK backend has to prevent such unauthorized writes; it can do so via static analysis [50], runtime checks [22] or page-table sealing [36].

In addition, the MPK backend introduces isolation requirements for the scheduler and the Memory Manager (MM): the scheduler holds the value of the PKRU for threads that are not currently running, and so its memory is as critical as the PKRU register itself. The MM’s domain includes the page-table holding the mapping between pages and protection domains. This implies that the scheduler and MM have to be trusted when using MPK. In our implementation we use a provably correct scheduler implemented in Dafny, and we can also use SH to harden schedulers/MMs implemented in C.

Our MPK backend supports two types of gates. In the `shared-stack` gate, heap and static memory are isolated and only shared data is accessible from all compartments in dedicated heap/static memory segments. Thread stacks are located in a domain shared by all compartments. This gate is similar to ERIM’s [50]. With the `switched stack` gate, the heap, stacks, and static memory are all isolated. There is one stack per thread per compartment and the stack is switched at domain boundaries. Parameters are copied to the target domain stack, and shared stack data is placed on a shared heap. This gate is similar to HODOR’s [22].

**VM-based Backend.** Many works use virtualization to support isolation within a kernel [33, 40, 41, 56]. VM-based isolation provides strong security guarantees and is widely supported, at the cost of higher overhead.
Our toolchain generates one VM image per compartment. Images contain the minimum set of micro-libraries necessary to run the VM independently (platform code, memory allocator, scheduler), along with a thin RPC implementation based on inter-VM notifications and a shared area of memory for shared heap/static data. It is mapped in all compartments (VMs) at an identical address so that pointers to/in shared structures remain valid. Components do not share a single address space anymore, and run on different vCPUs. Hence, each compartment needs its own memory allocator and scheduler, so these have to be trusted. Our VM-based isolation backend is currently based on Xen, with KVM support underway.

**SH Support.** FlexOS’s SH support is modular: we can apply hardening mechanisms per compartment (not system-wide), allowing for fine-grained protection and performance trade-offs. For example it is possible to apply SH only to components that interact directly with the outside world, such as the network stack. Our implementation supports KASAN, Stack protector and UBSAN on GCC, and CFU and SafeStack under clang. A key requirement for SH is the ability to have a separate memory allocator per compartment: as many SH techniques instrument malloc, using a single global allocator would result in the entire system paying the cost of the instrumented allocator. FlexOS can be configured to use separate memory allocators per compartment to avoid such overheads when only a subset of compartments are hardened.

<table>
<thead>
<tr>
<th>Component</th>
<th>SH: all but C</th>
<th>SH: C only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler</td>
<td>496Mb/s</td>
<td>2.90 Gb/s</td>
</tr>
<tr>
<td>Network stack</td>
<td>631Mb/s</td>
<td>2.76 Gb/s</td>
</tr>
<tr>
<td>LibC</td>
<td>1.47Gb/s</td>
<td>1.25 Gb/s</td>
</tr>
<tr>
<td>Rest of the system</td>
<td>1.08Gb/s</td>
<td>2.50 Gb/s</td>
</tr>
<tr>
<td>Entire system</td>
<td>2.94Gb/s (baseline)</td>
<td>489 Mb/s</td>
</tr>
</tbody>
</table>

**4 Preliminary Results**

We studied the performance impact brought by a number of FlexOS’ configurations for two apps: an iperf server and Redis. We aim to confirm that FlexOS allows easy exploration of a wide design space of security/performance trade-offs: each configuration is obtained by setting a few options and recompiling the LibOS against the app sources. Both apps were manually ported to the prototype, though most of this process should be easy to automate. Experiments were run on a Xeon Silver 4110 (2.1 GHz), with KVM and Xen.

**Safe iperf.** In our first test, we created an iperf server where an untrusted network stack is isolated from the rest of the OS image. We test three configs: 1) two compartments with MPK, one for the stack and one for rest of the OS; 2) separate VMs for the two compartments; 3) A single compartment, with SH applied only to the network stack.

Performance results as measured by an iperf client are shown in Fig. 3. At the server side, we vary the size of the buffer passed to recv. With SH and MPK, for small buffers there is a non negligible slowdown (2x to 3x). However, these solutions catch up quickly to the baseline, yielding similar performance starting at 1KB buffer size. Xen’s numbers are lower due to Unikraft not being optimized for this hypervisor; still, we observe that the payload needs to be larger for the VM backend to catch up to the baseline, 32KB, due to increased domain switching costs. These results show that the performance impact of various protection mechanisms depends on the workload, so locking into a protection mechanism at design time is suboptimal.

**iperf: Fine-Grained SH.** FlexOS’ modular design allows us to enable/disable SH at micro-library granularity. We ran iperf with a variable number of FlexOS’ components running with SH: the network stack, the scheduler, the standard C library (LibC), and the rest of the system including iperf itself.

Results are in Table 1. The performance impact strongly depends on the component running with SH: the scheduler brings a 1% overhead while the LibC has a 2.3x slowdown. Interestingly, the slowdown with SH for the network stack is low (6%). SH for the entire system has a 6x slowdown, demonstrating the benefits of FlexOS’ flexibility, useful in scenarios where components have variable levels of trust and variable performance impact when protected with SH.

**Redis: Isolation Strategies.** We ran Redis in various scenarios. We defined 4 compartmentalization models: (NW stack, rest of the system){NW stack, scheduler, rest of the system} (NW only), (NW stack, scheduler, rest of the system) (NW/sched/rest), (NW stack + scheduler, rest of the system) (NW and sched/rest), and a baseline with no isolation. These demonstrate FlexOS’ capacity to seamlessly manage various trust models. For MPK we ran both the shared and switched stack versions.

The results are in Figure 5. The isolation overhead depends on the number of compartments and how they communicate. Isolating only the network stack brings on average a 17% slowdown, while also isolating the scheduler brings a 1.4x (shared stack) and 2.25x (switched stack) slowdown – an increase due
to the stack switch overhead. This points to frequent communication between the scheduler and the network stack, making intensive use of wait queues through semaphores. However, putting the network stack and the scheduler in the same compartment does not increase performance: this is due to semaphores being implemented in another compartment (LibC). This brings the need for further compartmentalization or redesign of the components. Similar to iperf, the isolation overhead drops significantly when the request size increases.

Redis: SH. We ran Redis enabling SH for the network stack with 1) a global allocator for the entire system and 2) a dedicated local allocator for the network stack and another for the rest of the system. The results are in Figure 4. With a global allocator, the slowdown from running the network stack with SH is on average 1.45x. FlexOS’ capacity to easily setup a local allocator for the network stack allows us to reduce that overhead to a 1.24x slowdown. Overall, the results for Redis show that FlexOS can manage a wide range of security/performance requirements scenarios.

Verified Scheduler. We developed a verified cooperative scheduler written in Dafny [31]; the scheduler’s safety is given by pre- and post-conditions that are statically proven to hold by Dafny. We generate C++ code from the scheduler and integrate it in FlexOS by adding glue code. How can we embed this safely alongside untrusted code? To protect the scheduler’s memory from external writes we can either apply SH to the rest of the unikernel or use MPK. To check that pre-conditions hold on call we integrate the checks in the glue code, and disable interrupts. In future work we will generate glue code automatically.

The context switch latency of our verified scheduler is 218.6ns, 3x slower than the C scheduler (76.6ns). This is fairly high, but Fig. 4 shows that the verified scheduler’s overhead over the C one is always below 6% for Redis.

5 Open Questions

Decoupling OSes isolation and safety primitives from their fundamental design brings a number of challenges.

How to minimize porting effort? FlexOS requires porting, not only for kernel-internal libraries, but also for external user-space libraries. This porting process usually boils down to identifying shared data and handling indirect cross-component calls, a common effort among isolation frameworks [21, 38]. While it is a one-time, reasonably inexpensive effort, we recognize that it might hinder the adoption of our approach [43]. Further, manual approaches are not fail proof and can result, for example in over- or under-sharing data. To address these issues, automated porting techniques, mostly explored at the user-space level [6, 35, 48], can be explored.

Another element of the porting process is the writing of per-library metadata. These metadata are used by the design space exploration tool to automatically derive a compartmentalization strategy. The tool is then able to guarantee that properties hold according to the specified characteristics of each component. The resulting kernel is guaranteed to be correct as long as the metadata themselves are correct. But who verifies the specification/metadata? The process of writing metadata is error prone, and methods for (semi-)automatically generating them should be explored.

Isolation alone is not enough. Traditional system call APIs are designed from the outset as a trust boundary. Not only are they copy-based and carefully check function arguments, they are also designed as to avoid more subtle privilege escalation vulnerabilities, e.g. confused deputies. For such APIs, swapping the isolation mechanism (e.g., from standard system calls to MPK domain switching) is relatively straightforward.

On the other hand, when the API was previously developed without a trust model (as is the case with all kernel internal APIs, but also userland library APIs), introducing isolation is a more complex task; isolation alone is not enough, and in order to provide protection against a wide range of attacks, APIs have to be carefully revisited [11]. Further, in the case of FlexOS, we only want to execute such checks when they are really needed, depending on the instantiated kernel configuration: if component A is together with component B in the same trust domain, then checks are not necessary, but they are when component C (in another domain) calls component B.

A possible approach to tackle this problem is the one that we envision to take for preconditions: by enriching all micro-libraries with API metadata, the build system could possess sufficient information to automatically generate wrappers that would include or exclude these checks on-demand.

6 Related Work

Previous work addressed the isolation inefficiencies of monolithic kernels by reducing the TCB through separation [4, 44] and micro-kernels [20, 24]. More recently, OSes providing security through software isolation brought by safe languages [7, 13, 25, 36, 39] have been proposed. In SASOSes, isolation has been provided with traditional page tables [10, 23, 32] and recently through intra-address-space hardware isolation mechanisms [34, 42, 45, 47]. Formal verification offers deterministic security guarantees, but has trouble scaling to modern OSes’ large codebases [28, 29]. Low-overhead runtime protection mechanisms are commonly found in production kernels [15, 17]. However, the most security-efficient
ones [16] are only enabled for test runs [51] due to their high performance impact.

In all, each of these approaches represents a single point in the OS design space and lacks the flexibility of FlexOS to automatically configure variable, fine-grained security/performance profiles. LibrettOS [41] does allow a LibOS to switch between SASOS and microkernel modes, but remains limited to a small subset of the security/performance design space. SOAAP [21] proposes a system to explore software’s compartmentalization space using static/dynamic analysis; however, this work targets monolithic user-space code-bases, as opposed to modular kernel code-bases for FlexOS.

7 Conclusion and Future Work

FlexOS provides developers the ability to mix and match isolation primitives, be they hardware or software, which allows creating tailor-made versions of the same app for target workloads, with good performance and improved security, as our experiments have shown for two apps.

This paper is only an initial exploration of the potential benefits of FlexOS. Our future work aims to automate checking the safety of a proposed configuration, and searching for configurations with desired properties automatically. This will in turn enable developers to build robust software by mixing and matching components with various trust levels.

Acknowledgments

We would like to thank the anonymous reviewers for their comments and insights. A special thanks goes to Julia Lawall for her help on Coccinelle. This work was partly funded by the New Investigator Award grant EP/V012134/1, as well as the UK’s EPSRC grants CORDION and 758815 (CORNET), as well as the EU H2020 grant agreements 825377 (UNICORE), 871793 (AC-IT), 891710 (FORTE), and 871707 (ACCORDEON) and 758815 (CORNET), as well as the UK’s EPSRC grants CORDION and 758815 (CORNET), as well as the EU H2020 grant agreements 825377 (UNICORE), 871793 (AC-IT), 891710 (FORTE), and 871707 (ACCORDEON) and 758815 (CORNET).

References


85


