Proving full-system security properties under multiple attacker models on capability machines

Thomas Van Strydonck, Aina Linn Georges, Armaël Guéneau, Alix Trieu
Aarhus University

Amin Timany, Frank Piessens, Lars Birkedal, Dominique Devriese
Aarhus University, KU Leuven, Vrije Universiteit Brussel

Abstract—Assembly-level protection mechanisms (virtual memory, trusted execution environments, virtualization) make it possible to guarantee security properties of a full system in the presence of arbitrary attacker provided code. However, they typically only support a single trust boundary: code is either trusted or untrusted, and protection cannot be nested. Capability machines provide protection mechanisms that are more fine-grained and that do support arbitrary nesting of protection. We show in this paper how this enables the formal verification of full-system security properties under multiple attacker models: different security objectives of the full system can be verified under a different choice of trust boundary (i.e. under a different attacker model). The verification approach we propose is modular, and is robust: code outside the trust boundary for a given security objective can be arbitrary, unverified attacker-provided code. It is based on the use of universal contracts for untrusted code: sound, conservative contracts which can be combined with manual verification of trusted components in a compositional program logic. Compositionality of the program logic also allows us to reuse common parts in the analyses for different attacker models. We instantiate the approach concretely by extending an existing capability machine model with support for memory-mapped I/O and we obtain full system, machine-verified security properties about external effect traces while limiting the manual verification effort to a small trusted computing base relevant for the specific property under study.

I. INTRODUCTION

Assembly-level security primitives are a cornerstone of secure systems, and they come in many forms. CPU-supported security mechanisms like virtual memory, trusted execution environments, virtualization, micro-policies or capability machines all offer a form of encapsulation, which supports the execution of untrusted code with restricted authority. Some architectural security mechanisms, such as virtual memory, virtualization or trusted execution environments, are carefully optimized for specific security abstractions, such as processes, virtual machines or enclaves, and provide poor support for features which fall outside of these abstractions. In this paper, we are interested in such a feature, which is poorly supported by the most-used security mechanisms: nested encapsulation. This refers to scenarios where an encapsulated piece of code (e.g. a user process or virtual machine) further encapsulates a subset of its own code from the rest of its code. When nested encapsulation is poorly supported by the architectural primitives, it can only be supported at the cost of additional effort, complexity and a certain performance loss. For example, library OSs like Graphene require host OS cooperation to implement process isolation [1] and running virtual machines inside virtual machines requires additional context switches with additional overhead [2].

Contrary to many other primitives, micro-policies [3] and capability machines [4], [5], [6] are designed explicitly for generality and flexibility. In particular, capability machines offer good support for nested encapsulation, as we now explain. On a capability machine, capabilities are used to represent authority explicitly. Different forms of capabilities represent authority over memory, the authority to invoke other code, etc. Unprivileged code can easily set up an encapsulation boundary by constructing an object capability: an opaque capability that can be invoked by other code and only makes private state available after invocation. This private state can in turn include other capabilities representing additional authority. An object capability invocation hence represents a context switch between security domains.

Building on related work in high-level languages [7], [8], [9], Skorstengaard et al. and Georges et al. have developed a methodology for robust modular verification of software running on capability machines [10], [11] that supports proving (security) properties in the presence of untrusted code. The idea is to formalize the hardware-provided security guarantees in the form of a universal contract: a separation logic contract that holds for arbitrary, untrusted code on the machine. This universal contract expresses a form of capability safety: the untrusted code’s authority is effectively bounded by the authority of the capabilities it is given access to. In robust modular verification, the program logic allows combining manual verification of a property for certain components with this universal contract for untrusted code to obtain a full-system proof of the property.

For now, this work has remained restricted to proving artificial security properties: for example the fact that an assertion failure flag will never be set [11], [12] or equi-termination of programs [13]. In this paper, we extend this robust modular verification approach to a capability machine with memory-mapped I/O (MMIO). Although this is not technically the most complex feature to add, it does allow us to prove end-to-end system properties that are more interesting and realistic. Contrary to the artificial properties of previous work, our results specify that a security property holds for
writes to peripheral MMIO addresses need to be replaced with invocations of the wrappers.

A security analysis of nested wrappers should consider different attacker models, for example the four models depicted in Fig. 2. These diagrams, gray components are treated as untrusted: white components are manually verified for correctness and security (i.e. proper encapsulation towards the gray components). For example, a security analysis of wrapper \( w_1 \) could use the leftmost model: only wrapper \( w_1 \) is trusted and all other code on the system is treated as arbitrary. Because of the machine’s capability safety, it suffices to manually verify the wrapper and its encapsulation to verify the intended property. A second analysis could use the attacker model of Fig. 2b in addition to wrapper \( w_1 \), it relies on the secure wrappers \( w_{21} \) and \( w_{22} \). This second analysis has a larger TCB but can prove the stronger properties that \( w_{21} \) and \( w_{22} \) enforce. The analysis does not inspect the code of wrapper \( w_1 \) for this, but relies on a functional contract for it (perhaps provided by the hardware manufacturer together with \( w_1 \)). Further analyses could use additional attacker models as depicted in Fig. 2c and Fig. 2d.

Note that while the system is analyzed several times, we hasten to point out that (1) only wrapper code is manually verified and (2) no wrapper is verified twice: \( w_1 \) is verified manually, resulting in a functional correctness contract, which is then used when manually verifying \( w_{21} \) and \( w_{22} \). The full system properties are obtained by combining the verification results of each of the wrappers with our general capability safety theorem. Note also that although \( w_{21} \) and \( w_{22} \) are both trusted in the second attacker model, compositionality of our program logic still allows us to verify them separately, relying on a contract for each other’s behavior. This avoids creating unnecessary dependencies when verifying wrappers.

In this paper, we present and explain our approach by considering representative example wrappers on a model capability machine. A first example corresponds roughly to the first two layers of Figure 1 with wrappers enforcing a simple bounds check and a maximum bound on the amount of accesses respectively (i.e. a stateful property). In this first example, we demonstrate that we can modularly reason about independent wrappers and that the verification effort can be shared when they are implemented according to a fixed code structure. Our second example shows that our approach also supports more complex properties that consider interactions with several peripherals. It considers a setup where \( w_{22} \) is replaced with a wrapper \( w_{22\_bis} \) that limits the rate at which a certain peripheral is accessed. \( w_{22\_bis} \) will only allow accesses to its peripheral after an external timer device indicates that sufficient time has passed. It does not follow the same fixed structure as the first wrappers and is verified separately.

To summarize, our contributions are the following:

- We extend the capability machine model, program logic and logical relation of Georges et al. [11] with memory-mapped I/O and secure enforcement of I/O properties and reprove
their universal contract for arbitrary code on the machine.
- We demonstrate universal contracts for proving full-system security properties on effect traces in the presence of untrusted code, thus obtaining more interesting and realistic end-to-end properties.
- We extend the approach to systems with nested encapsulation by analyzing the same system several times with different attacker models.
- We apply this approach to nested policy enforcement wrappers around peripherals and obtain machine-checked full-system proofs of the different stakeholders’ intended properties. Custom separation logic resources and wrapper specifications in so-called HOCAP style allow us to accurately specify the contracts between wrappers and verify them modularly. We demonstrate that verification effort can be shared for wrappers sharing a fixed code structure.

All of our proofs have been machine-verified in Coq, using the Iris program logic, and are available online.

II. A simple capability machine with MMIO support

First, we present the operational semantics of our capability machine. Our work builds upon the work of Georges et al. [11] and, transitively, on that of Skorstengaard et al. [10], [12]. As such, our presentation here is similar to theirs, though simplified to fit our purposes. Specifically, we do not consider so-called local and uninitialized capabilities.

Section II-A presents the operational semantics for a simple capability machine and Section II-B explains how we add memory-mapped I/O. The semantics is summarized in Fig. 4 to 6 with additions for memory-mapped I/O in blue.

A. A simple capability machine

The syntax of capability machine programs is given in Fig. 3. We consider a machine with finite memory bounded by AddrMax. A machine word \( w \in \text{Word} \) is either an unbounded integer or a capability. A capability is a quadruple \( (p, b, e, a) \) representing a permission \( p \) with authority over range \( [b, e) \) and currently pointing to address \( a \). A permission is an element of the lattice depicted in Fig. 4. There are six different permissions: opaque (O), enter (E), read-only (RO), read/execute (RX), read/write (RW) and read/write/execute (RWX). These permissions are standard, except for the opaque permission which provides no privilege and the enter permission, inspired by the M-Machine [5], that can be used to build opaque closures or object capabilities. Enter capabilities are “unsealed” into read/execute capabilities when jumped to. The capability is then available in the pc register and can be copied into another register to restore environment variables in the case of a closure.

Fig. 4 defines the small-step operational semantics of the machine. The machine’s state consists of an execution mode \( \mu \) and an execution configuration \( \varphi \). The mode \( \mu \) models the machine’s instruction cycle, which loops infinitely (expressed by Repeat \( \mu \)) until it reaches a successful done state Done Halted through RepeatHalt or a failed state Done Failed through RepeatFail. The RepeatSingle rule allows for the execution of single instructions through the Execute rule. If the execution of the instruction is successful, i.e. execution in Execute does not fail or halt and results in a Done SingleStep state, then RepeatStandby allows for another iteration of the processor’s instruction cycle.

An execution step (Execute) requires an executable, in-range capability \( (p, b, e, a) \) in the pc register. The word \( z \) at address \( a \) is then read and decoded into an instruction \( \text{decode}(z) \) which is executed on the current configuration \( \varphi \) to result in a new machine state \( \llbracket \text{decode}(z) \rrbracket(\varphi) \). Machine instructions \( i \) operate over registers \( r \) or either integers or registers \( \rho \). The behavior of instruction \( i \) in configuration \( \varphi \) is specified by \( \llbracket i \rrbracket(\varphi) \) defined in Fig. 5. Most instructions use the auxiliary function updPC to increment the pc register at the end of their executions. Since the address space is finite, pointer arithmetic such as \( a + 1 \) can fail. For ease of reading, we write \( a + k \) to indicate successful pointer arithmetic.

Instructions fail and halt respectively terminate the execution in a Failed or Halted state. move \( r \rho \) copies \( \rho \) (its value if it’s an integer, or its contents if it’s a register) into \( r \). Memory can be manipulated using the load and store instructions: load \( r_1 r_2 \) reads the value at the address pointed to by the capability in \( r_2 \) assuming it has read permission and is within bounds, and copies the value into \( r_1 \). Similarly, store \( r \rho \) stores \( \rho \) at the address pointed to by the capability in \( r \) assuming it has write permission and is within bounds. The jmp instruction jumps to a capability, by writing it into the pc register. As explained earlier, the jmp instruction unseals E capabilities into RX capabilities before jumping to them.
\[
\begin{align*}
   a & \in \text{Addr} \quad \triangleq [0, \text{AddrMax}] & EventTy & \triangleq \text{IOWrite} \mid \text{IRead} \\
p & \in \text{Perm} \quad \triangleq \{ \text{O} \mid \text{E} \mid \text{RO} \mid \text{RX} \mid \text{RW} \mid \text{RWX} \} & e & \in \text{Event} \quad \triangleq \text{EventTy} \times \text{Addr} \times \text{Z} \\
c & \in \text{Cap} \quad \triangleq \{(p, b, e, a) \mid b, e, a \in \text{Addr}\} & t & \in \text{Trace} \quad \triangleq \text{list Event} \\
w & \in \text{Word} \quad \triangleq \text{Z} + \text{Cap} & \varphi & \in \text{ExecConf} \quad \triangleq \text{Reg} \times \text{Mem} \times \text{State} \times \text{Trace} \\
r & \in \text{RegName} \quad \triangleq \{ p \mid r_0 \mid r_1 \mid \ldots \mid r_{31} \} & \delta & \in \text{DoneState} \quad \triangleq \text{Standby} \mid \text{Halted} \mid \text{Failed} \\
reg & \in \text{Reg} \quad \triangleq \text{RegName} \rightarrow \text{Word} & \mu & \in \text{ExecMode} \quad \triangleq \text{SingleStep} \mid \text{Repeat} \mu \mid \text{Done} \delta \\
m & \in \text{Mem} \quad \triangleq \text{Addr} \rightarrow \text{Word} & \varphi & \in \text{Z} + \text{RegName} \\
i & ::= \text{jmp} \ r \mid jnz \ r \mid \text{move} \ r \rho \mid \text{load} \ r \ r \mid \text{store} \ r \ \rho \mid \text{add} \ r \ \rho \ \rho \mid \text{sub} \ r \ \rho \ \rho \mid \text{eq} \ r \ \rho \ \rho \mid \text{lt} \ r \ \rho \ \rho \mid \text{lea} \ r \ \rho \mid \text{restrict} \ r \ \rho \mid \text{subseg} \ r \ \rho \ \rho \mid \text{isptr} \ r \ r \ | \text{getp} \ r \ | \text{getb} \ r \ | \text{gete} \ r \ | \text{geta} \ r \ | \text{fail} | \text{halt}
\end{align*}
\]

Figure 3: Machine words, machine state and instructions.

\[
\begin{align*}
   \text{updPC}(\varphi) &= \left\{ \begin{array}{ll}
            \text{(Done Standby, } \varphi[p, b, e, a + 1]) & \text{if } \varphi.(\text{pc}) = (p, b, e, a) \\
            \text{(Done Failed, } \varphi) & \text{otherwise}
            \end{array} \right. \\
   \text{getWord}(\varphi, \rho) &= \left\{ \begin{array}{ll}
            \rho & \text{if } \rho \in \text{Z} \\
            \varphi.(\text{reg}(\rho)) & \text{if } \rho \in \text{RegName}
            \end{array} \right. \\
   \text{updST}(\varphi, e, s) &= \varphi[\text{state} \rightarrow s][\text{trace} \rightarrow \varphi.\text{trace} \mapsto [e]]
\end{align*}
\]

Figure 5: Operational semantics: instruction semantics.

\[
\begin{align*}
   \text{REPEAT} & \text{SINGLE} \quad (\text{SingleStep, } \varphi) \rightarrow (\text{Done } \delta, \varphi') \\
   \text{REPEAT} & \text{STANDBY} \quad (\text{Repeat } (\text{Done Standby}), \varphi) \rightarrow (\text{Repeat } (\text{Done } \delta), \varphi') \\
   \text{REPEAT} & \text{HALT} \quad (\text{Repeat } (\text{Done Halted}), \varphi) \rightarrow (\text{Repeat } (\text{Done Step}), \varphi) \\
   \text{EXEC} & \text{SINGLE} \quad \left\{ \begin{array}{ll}
            \llbracket \text{decode}(z) \rrbracket(\varphi) & \text{if } \varphi.(\text{pc}) = (p, b, e, a) \wedge b \leq a < e \wedge \\
            \rho \in \{ \text{RO, RX, RWX} \} \wedge \varphi.(\text{mem}(a)) = z & \text{otherwise}
            \end{array} \right.
\end{align*}
\]

Figure 6: Operational semantics: reduction steps.
Capabilities can be modified using the restrict, subseg and lea instructions. restrict can be used to decrease the permission of a capability according to the permission lattice’s partial order ≲. subseg can be used to decrease the range of authority of a capability, while lea can be used to modify where a capability points to. As E capabilities are used to encapsulate code and data, they cannot be modified unless they are unsealed, hence the instructions subseg and lea fail when used with E capabilities. Indeed, e.g. changing the address of an E-capability could enable Return Oriented Programming (ROP) flavored attacks [12]. Instructions to read capabilities’ fields are also provided: geta, getp, getb and gete respectively read the \(a, p, b\) and \(e\) fields of a capability \((p, b, e, a)\). Not shown in Fig. \(5\) are instructions jnz (conditional jump), add, sub (addition and subtraction), eq (equality), lt (comparison) and ispsect to check whether a register contains a capability. Finally, if none of the above cases apply, the execution falls through to a failed state as shown on the last row in Fig. \(5\).

### B. Adding support for memory-mapped I/O

To allow communication between the CPU and devices, we add support for MMIO. Those operations are indicated in blue in Fig. \(3\) and \(5\). For simplicity, we do not yet support interrupts; the CPU and devices must poll memory for updates. We discuss adding interrupts in Section \(VI\).

To model MMIO, we assume a set \(\mathbb{MMIO}\) of addresses reserved for MMIO and augment execution configurations \(\varphi\) with a trace \(t\) of MMIO events \(e\), and an environmental state \(s\) drawn from a set \(\text{State}\) as shown in Fig. \(3\). An event \(e\) is a triple of a mode \(e\.\text{type}\) (read or write), an address \(e\.\text{addr}\), and an integer \(e\.\text{value}\) that is read or written. The operational semantics of our machine in Fig. \(5\) is parameterized by this set \(\text{State}, \mathbb{MMIO}\) and two operations \(\text{mmioLoad} : (\text{State} \times \text{Addr}) \rightarrow (\text{State} \times \mathbb{Z})\) and \(\text{mmioStore} : (\text{State} \times \text{Addr} \times \mathbb{Z}) \rightarrow \text{State}\), that model how the state of the devices reacts to MMIO loads and stores.

Fig. \(5\) shows the new behavior of load and store for MMIO addresses. load will use mmioLoad to get the value at address \(a\) from the environment and load it into the register. Similarly, store uses mmioStore to indicate that a value is written at some address. In both cases, the operations transition the environment’s state and an IORead or IOWrite event is recorded in the trace.

### III. Example wrappers

This section details the two examples with nested parapass-through security wrappers that were described in the introduction. The goal is to illustrate how stakeholders such as the ones in Fig. \(1\) can set up the capability machine to achieve their security objectives.

#### A. Three-layer stateful example with orthogonal wrappers

The first system we consider is setup as in Fig. \(1\) with an additional bottom-most wrapper \(\text{wrapper}_0\). There are hence 3 layers of simple wrappers, where the third layer contains two disjointly operating wrappers. The proof effort for this example can be shared, since the wrappers share a common structure, as will be discussed in section \(IV-D\). The different wrappers enforce the following concrete invariants, modelling the kind of real security properties we discussed in the introduction:

- **Wrapper\(_0\)** encapsulates all of MMIO, and creates a read and write closure for MMIO that higher-level wrappers use. It does not enforce its proper predicate, i.e. it enforces the trivially true predicate \(P_0\) on the trace \(t\) in Fig. \(7\). We separate this wrapper from the others, since its implementation deviates: it is the only wrapper that does not recursively call another wrapper, but rather accesses MMIO directly.

- **Wrapper\(_1\)** ensures that no more than 1000 MMIO-events (read and write combined) occur once the capability machine boots. This invariant is expressed by the predicate \(P_1\) on the trace \(t\) in Fig. \(7\).

- To ensure safety of values sent to their respective peripherals, wrapper\(_{21}\) solely allows positive values, whereas wrapper\(_{22}\) solely allows negative values. Note that it would be trivial to extend this to an arbitrary bounds check. This is expressed by \(P_{21}\) and \(P_{22}\) in Fig. \(7\) where \(\uparrow_{21}(P_{21})\) is a predicate on traces that holds on a trace \(t\) iff \(P_{21}(e)\) holds for all events \(e\) in \(t\).

- We model two different peripherals (e.g. network and display) situated at the memory-mapped addresses \(a_1\) and \(a_2\), respectively. Wrapper\(_{21}\) only allows events destined for address \(a_1\), i.e., \(\text{wrapper}_{21}\) enforces predicate \(P_{21}\) on a filtered view of the general MMIO trace. The filtering is represented by \(F_{21}\) in Fig. \(7\). Thus \(\text{wrapper}_{21}\) enforces \(P_{21} \circ F_{21}\) on the MMIO trace. Analogously, \(\text{wrapper}_{22}\) enforces \(P_{22} \circ F_{22}\). The complement filter \(\overline{F}_2\) will be used to prove that no addresses other than \(a_1\) and \(a_2\) receive MMIO events, by requiring that \(\overline{F}_2(t) = \{\}\).

The previous description has provided us with sufficient details to define the verification goals of each stakeholder. These goals are formulated as security objectives, and summarized in Fig. \(6\). Note that wrapper\(_0\) does not have any security objective of its own, since it solely encapsulates MMIO. \(\text{Obj-1}\) specifies the guarantees that wrapper\(_1\) hopes to achieve from verification. \(\text{Obj-1}\) states that if the initial memory \(m_0\) and registers \(r_0\) constitute a valid configuration \(\text{init}_\text{config\_1}(r_0, m_0)\) (further explained below), then any execution starting from the empty trace \(\emptyset\) and an arbitrary state \(s_0\) and taking an arbitrary number of steps (denoted by \(\rightsquigarrow\)), will result in a configuration that has a trace \(t'\) satisfying \(P_1\). In other words, \(\text{wrapper}_1\) can be sure that \(P_1\) will hold on any trace of execution, as long as the capability machine boots into a configuration satisfying \(\text{init}_\text{config\_1}\).

For the second layer, we get two separate security objectives; \(\text{Obj-21}\) and \(\text{Obj-22}\). This models the situation where the two drivers are developed and verified independently (perhaps by separate developer teams in the same company), relying on a contract for the other wrapper, rather than its exact code. Otherwise, \(\text{Obj-21}\) and \(\text{Obj-22}\) are analogous to \(\text{Obj-1}\). They enforce that if the initial memory and register configuration is satisfactory, the respective predicates \(P_{21}\) and \(P_{22}\) hold over the network and display parts of the final trace \(t\), i.e. \(P_{21}(F_{21}(t))\) and \(P_{22}(F_{22}(t))\) hold. Additionally, the complement filter \(\overline{F}_2\)
The memory layout contains 3 major parts; code for the wrapper of view of wrapper, MMIO wrappers in each layer before passing control to the adversary.

Fig. 7 graphically illustrates these assumptions for wrappers 1 and 21 (22 is analogous). The figure also summarizes the different components involved in correctly setting up the memory from containing any capabilities; a conservative assumption made for simplicity reasons, to avoid a trivial bypass of the encapsulation of trusted components. Additionally, the value in PC register is initialized correctly, and disallows the adversary’s capability to point to Set-up Code 0 and contains an omnipotent capability.

The purpose of the set-up code is to initialize the wrapper code, and adversarial code. The MMIO region represents all of MMIO, and is unique to wrapper0, since no other wrappers access MMIO directly.

The code of wrapper0 itself consists of a read closure from address \( d_{-r0} \) to \( d_{-w0} \), a write closure from \( d_{-w0} \) to \( d_{-ls0} \) and local state used by the closures, from \( d_{-ls0} \) to \( d_{-e0} \). As mentioned before, the read and write closures do not enforce any predicate on the trace; they simply provide read and write functionality to MMIO memory. The local state consists of a single address, which the set-up code will store a capability (\( RW, MMIO_b, MMIO_c, MMIO_d \)) for MMIO into. It is hence independent of the current trace, and given by \( LS_{-gen1} \) in Fig. 7. This capability provides the read and write functionality to MMIO memory.

In order to simplify wrapper invocations, we settled on the following common calling convention in our examples:

- \( r\texttt{reqint} \) succeeds iff \( r \) contains an integer
- \( \texttt{lea}_{-a} r \rho r_{aux} \): absolute version of \( \texttt{lea} \), that makes the capability in \( r \) point to the address corresponding to \( \rho \)
- \( \texttt{rclear} \tau \): clears the set of registers \( \tau \) by overwriting them with the value \( 0 \).
Figure 9: The memory layout from the point of view of wrappers 0, 1 and 21. Verified parts of memory are shown in green, regions that the wrapper’s set-up code assumes correctness contracts for are shown in blue, and adversarial code is shown in red. Red dashed lines illustrate how each following wrapper is situated in the adversarial region of the previous wrapper. Blue dashed lines show how an abstract view of the previous memory layout is assumed in the following wrapper.

Figure 10: The flow of control and a few representative register states when jumping to the adversary in the execution of the motivating example. Black dotted connectors indicate register state during the indicated transition. Gray connectors indicate that the pointed-to registers received the indicated value in the previously executed set-up code.

Figure 11: The code for wrapper0’s write closure (Write Wrapper 0 in Fig. 9a).

Figure 12: The set-up code for wrapper0 (Set-up Code 0 in Fig. 9a).

The set-up code starts by deriving the previously discussed MMIO capability from the omnipotent pc, and storing it at address d_0. Next, it

wrapper code is assumed pre-loaded in memory, but initial memory cannot contain any capabilities. The set-up code starts by deriving the previously discussed MMIO capability from the omnipotent pc, and storing it at address d_0. Next, it
derives the read and write closures from the pc and stores them in \( r_1 \) and \( r_2 \). Lastly, it restricts the omnipotent pc to the adversary region, clears all auxiliary registers and jumps to the adversary, thereby loading \( r_0 \) into the pc. Fig. 10 demonstrates how execution starts in Set-up Code 0, and how, when jumping to Adversary 0, pc, \( r_1 \), and \( r_2 \) are set up as previously described. From the point of view of wrapper\( 0 \), the concrete code stored inside Adversary 0 is irrelevant, as capability safety ensures that no adversary will be able to bypass its read and write closures.

Let us now consider the memory layout for wrapper\( 1 \) in Fig. 9b. The layout is similar to Fig. 9a except for the topmost region. Since Set-up Code 0 gets to execute before passing control to Set-up Code 1, wrapper\( 1 \) assumes the existence of a region Layout 0, whose instructions satisfy a contract that captures the behavior of Set-up Code 0. Consequently, init_config\_1 in [Obj-1] requires the machine to boot inside the Layout 0 region and pass control to Set-up Code 1 at the end, with the register state as specified in Fig. 10. Requiring a contract rather than precise code makes the different layers more independent, and will, e.g., allow the hardware vendor to optimize network packet handling without affecting any proofs in higher-up layers.

The code for wrapper\( 1 \) is similar in layout, but makes use of more extensive local state than wrapper\( 0 \). Concretely, the read and write closures ensure that the local state always satisfies \( LS_1 \) in Fig. 7. \( LS_1 \) is defined in terms of a general local state \( LS_{gen} \). \( LS_{gen} \) describes the layout of local state for wrapper \( x \) (with \( x \neq 0 \)). It specifies that the first three addresses contain a rxw capability \( c_{\_ls2} \) for all of local state, and the read and write closures \( c_{\_pr(x)} \) and \( c_{\_wpr(x)} \), where \( pr(x) \) represents the layer-below wrapper, which \( x \) will call. For example, \( pr(22) = 1 \). Having \( c_{\_ls2} \) is required because jumping to an E capability in our capability machine results in a pc with rx permission, which disallows updating the local state. Lastly, \( LS_{gen} \) takes a list of custom values \( \tau_{cust} \) as an argument. This allows wrappers to specify additional local state to aid in enforcing their invariants. In this case, Fig. 7 defines \( LS_1 \triangleq \lambda LS_{gen} \cdot (\lfloor length(t) \rfloor) \), where \( x = 1 \) because wrapper\( r_1 \) requires access to its own local state, and \( pr(x) = 0 \) because wrapper\( r_1 \) will call wrapper\( r_0 \) to have it perform MWIO. Additionally, \( \tau_{cust} = [\lfloor length(t) \rfloor] \), because wrapper\( r_1 \) requires one extra address to store local state; a counter \( length(t) \) that corresponds to the number of MWIO events performed so far, to compare it to 1000.

Fig. 13 demonstrates how the read closure of wrapper\( r_1 \) uses local state. It makes use of a generic \texttt{read\_wrapper} template, which we use for any non-bottom-level wrapper in this example. The template uses a list of instructions \texttt{check\_read} to check whether the wrapper’s predicate (e.g., \( P_1 \) in this case) would still hold after the next MWIO event, and update the local state if this is the case. First, the template verifies whether \( r_0 \) is a valid address, and not just any integer. This is done using the \texttt{is\_addr} \( r_{aux1} r_{aux2} \) macro, which succeeds iff \( r \) contains an integer that corresponds to a memory address. Then, it calls upon the checking instructions. Lastly, it loads \( c_{\_r0} \) from address \( d_{\_ls1} + 1 \) and jumps to it. For wrapper\( r_1 \) the template is instantiated with \texttt{check\_1}, which checks that \( P_1 \) holds. These instructions first load \( c_{\_ls1} \) from \( d_{\_ls1} \), then load \( length(t) \) from \( d_{\_ls1} + 3 \), check whether \( length(t) + 1 < 1000 \) still holds, and fail if this is not the case. If the check fails, \( length(t) + 1 \) is stored to \( d_{\_ls0} + 3 \), ensuring that \( LS_1 \) holds again after the call to wrapper\( 0 \).

The set-up code for wrapper\( 1 \) is very similar to the code we discussed in Fig. 12. The only difference is that, rather than ensuring that \( LS_0([1]) \) holds, the set-up code needs to satisfy \( LS_1([1]) \) before jumping to Adversary 1. Fig. 10 again shows the state of key registers at that point.

Finally, Fig. 9c summarizes wrapper\( 21 \). Wrapper\( 21 \) again assumes a contract for lower-level wrappers, that is satisfied by the region Layout 0+1. This contract captures the behavior of Set-up Code 0 and 1 combined, i.e., the first two steps in Fig. 10. Similarly, a new region Layout 22 satisfies a second contract that captures the behavior of Set-up Code 22. Both contracts appear in the definition of init_config\_21 in [Obj-21] and enable more modular code development. We do not discuss wrapper\( 22 \) separately, since its layout is the dual of wrapper\( 21 \). Both wrappers share the same adversary.

The code for wrapper\( 21 \) itself is similar to the code for wrapper\( 1 \). It enforces \( LS_{21} \) in Fig. 7 which is again defined in terms of \( LS_{gen} \). No custom local state is needed to check \( P_{21} \). The set-up code is also similar, but it jumps to wrapper\( 22 \) before control is passed to Adversary 2, as shown in Fig. 10. This figure demonstrates how Set-up Code 21 sets up the closures for wrapper\( 21 \) in \( r_3 \) and \( r_4 \), whereas Set-up Code 22 (or in this case the assumed contract for Layout 22) sets up its closures in \( r_1 \) and \( r_2 \). Set-up Code 21 uses \( r_1 \) and \( r_2 \) to pass the closures for wrapper\( r_1 \) to Set-up Code 22.

**B. Rate limiting**

To demonstrate how the previous example generalizes to support a more complex property that requires interaction with multiple devices, we implemented and verified a second example where wrapper\( 22 \) is replaced by wrapper\( 22 \_bis \); a wrapper that implements rate limiting. The other wrappers and security objectives remain unchanged. Concretely, wrapper\( 22 \_bis \) relies on a trusted, memory-mapped timer device, and only allows an IO-event to or from its peripheral (at the same address \( \alpha_2 \) that wrapper\( 22 \) used) to occur when a value of 1 has been
read from the timer address \(a_{t}\) beforehand. In other words, \(\text{wrapper}_{22}\) enforces the predicate \(P_{22}\) in Fig. 14 on a version of the MMIO trace that has been filtered through \(F_{22}\). Here, the function \(\text{last}\) returns the most recent event in \(t\), if any. In summary, security objective \(\text{OBJ-22}\) is replaced by the following (where \(F_{2}^{2}\) now also disallows events to \(a_{t}\)):

\[
\text{Obj-22-bis} \quad \text{init-config}_{22}(r_{0}, m_{0}) \quad (r_{0}, m_{0}, 0, s_{0}) \rightarrow^{*} (r, m, t, s)
\]

To correctly enforce \(P_{22} \circ F_{22}\), wrapper\(_{22}\) consists of two different types of closures. First, a read and write closure similar to the ones demonstrated in Fig. 9 which clients can use to respectively read from and write to \(a_{2}\) if the last event in \(F_{22}(t)\) is a timer event that returned 1. Second, a read-only timer closure, which allows reading from \(a_{t}\) and returns the read value. To coordinate between these closures, they share local state that satisfies \(LS_{22}\) in Fig. 14.

The three closures uphold \(LS_{22}\) as follows:

- Whenever the timer closure is called, it writes a 1 to the local state if it read a 1 and 0 otherwise.
- Whenever the regular read or write closure is called, if the event is destined for address \(a_{2}\), it checks the local state to see if the stored value is 1. If not, the wrapper fails. If the value is 1, it is consumed and set to 0, and the call is passed on to wrapper\(_{1}\).
- Note that in our current set-up, wrapper\(_{22}\) is the sole wrapper that can read (and write) the timer address, since it requires a view of all MMIO events to \(a_{t}\) and \(a_{2}\) in \(F_{22}\). Section IV-A will discuss how our approach can be generalized to a setting where a closure is shared between multiple wrappers, e.g., wrapper\(_{21}\) and wrapper\(_{22}\).

IV. PROVING THE SECURITY OBJECTIVES

This section outlines the high-level technical ideas that underlie the proofs of security objectives such as the ones in Fig. 8. Intuitively, the proof of each wrapper’s security objective employs an invariant to state that the objective holds at each step of execution. Section IV-A discusses how each wrapper’s invariants are formalized in Iris.

Proving that the invariant always holds requires reasoning about 2 different phases of execution:

1) The wrapper’s concrete closures that we hand-verify should enforce the invariant, as Section IV-B further explains. Additionally, the concrete set-up code of the wrapper and (specifications for) the set-up code of all layer-below wrappers should respect the invariant. The latter is simple to prove, since set-up code does not perform IO itself.

2) The arbitrary adversarial code in the Adversary region should be safe to execute, i.e., have no way of bypassing the wrapper’s closures and breaking the invariant. Section IV-C discusses how we employ a semantic model to reason about the safety of unknown code in the capability machine.

In Section IV-D we finally discuss an approach to sharing the verification effort for wrappers that have a common structure. This is not required for our verification approach, but it allowed us to reduce the verification effort involved in proving the first example.

A. Invariants to enforce security objectives

In this section, we detail how each wrapper \(x\) employs invariants \(\text{inv}_{x}(t)\) to prove modularly that its security objective \(\text{OBJ-X}\) holds at each step of execution. It is insufficient to have an invariant that simply states that the security objective holds continuously. To be of general use, each wrapper requires three additional types of reasoning to be possible with its invariant.

First, each wrapper has a view of the physical trace, which is the part of the physical trace that it knows about. In our first example, wrappers 0 and 1 view the entire trace, whereas the views of wrappers 21 and 22 consist of all events addressed to \(a_{1}\) and \(a_{2}\), respectively. A wrapper \(x\) will only ever see a subview of the layer-below wrapper \(pr(x)\)’s view. By expressing the view of \(x\) in terms of the view of \(pr(x)\), the invariant ensures that all wrappers’ views are indeed recursively views of the actual physical event trace, obtained through repeated filtering.

Secondly, in case multiple wrappers \(x_{1}, \ldots, x_{n}\) have a common layer-below wrapper \(pr(x_{1})\), it should be possible to modularly reason about events they admit. For example, we should not have to know anything about the view of \(x_{n}\) on the trace, to reason about the view that \(x_{1}\) has on the trace.

Lastly, the invariant needs to ensure that any local state that the wrapper requires for its correct operation is enforced on the wrapper’s current view of the trace. For example, to prove correct operation of wrapper\(_{1}\) in our first example, the invariant must be able to guarantee that the number of MMIO events that wrapper\(_{1}\) keeps track of, is the number of events in the most up-to-date view of the trace.

In the remainder of this section, we flesh out these three types of reasoning by means of Fig. 15 which demonstrates how different aspects of the wrappers’ invariants help us achieve the desired reasoning. At the end, we showcase some concrete invariants used in our first example. Note that the enforcement of the security objective itself is trivially expressed by adding the condition \(P_{x}(t_{x})\) to the invariant, as Fig. 16 shows.

IV-A. Connecting \(x_{1}\) to \(pr(x_{1})\):

1) Connecting \(x_{1}\) to \(pr(x_{1})\): In general, a wrapper \(x_{1}\)’s view of the trace is a filtered view, a subsequence of the layer-below wrapper \(pr(x_{1})\)’s view. We can connect different
valid($F$) $\triangleq \exists P_e : \text{Event} \rightarrow \text{Prop.} \,(\forall t. \, F(t) = \text{filter}(P_e,t)) \land (\forall e : \text{Event} \, \text{decidable}(P_e(e)))$

orthogonal($F_1, F_2$) $\triangleq (\forall t. \, F_1(F_2(t)) = F_2(F_1(t)) = \emptyset)\,$

1) (filter_full $\gamma \, t \ast \text{filter_val} \, F \, t') \rightarrow F(t) = t'$

2) (filter_val $\gamma \, F \, t \ast \text{filter_val} \, F' \, t') \rightarrow \text{orthogonal}(F, F')

3) (\forall F', \text{valid}(F') \land \text{orthogonal}(F, F') \rightarrow F'(t) = F'(t'))

(flatfilter_full $\gamma \, t \ast \text{filter_val} \, F \, t'$)

3) Incorporating local state: While the security objective $P_e(t_e)$ has to be satisfied at each step of execution (i.e. atomically), the local state can temporarily be out of sync.

versa. Similarly, we might have multiple wrappers that only write certain ranges of output values, that only ever read, respectively write values, that always write specific pairs of MMIO values, etc. Note that orthogonality is more flexible than disjointness since it does not presuppose a notion of intersection, but that it degenerates to the latter in case we consider filters that filter on individual events (as is the case in our examples).

Given this notion of orthogonality, we defined a novel filter resource algebra (an Iris construct used to define custom separation logic resources) to reason about independent, orthogonal updates to a trace. The previous resources filter_full $\gamma \, t$ and filter_val $\gamma \, F \, t$ are in fact defined in terms of this resource algebra.

Fig. 15 defines the three most important properties that these two resources satisfy. First, we define a filter $F$ to be valid if it filters the trace by a decidable event predicate $P_e$. Property 1 states that $t'$ is indeed a view of $t$ through the filter $F$. Property 2 states that any two filter_val resources are guaranteed to be orthogonal. Property 3 then leverages orthogonality to express how we may update traces modularly: if all orthogonal, valid filters are unaffected by a trace update, then we can update a filter_full and filter_val without requiring ownership of any other filters. Fig. 16 illustrates how the filters $x_1, \ldots, x_n$ are connected to their common layer-below filter, assuming orthogonal filtering predicates.

The reader might wonder about the case where the views of $x_1, \ldots, x_n$ are not orthogonal. This case does not occur in our current examples, but Iris offers multiple resource abstractions that can be used to reason about different forms of shared views on the trace. For example, imagine a scenario where a clock closure (similar to the timer closure in our second example) is shared between wrapper$^{21}$ and wrapper$^{22}$, such that both wrappers can read timestamps from it and enforce their own predicates (e.g. “at least X seconds have to pass between any two writes to $a_2$”). The wrappers 21 and 22 would still require an orthogonal view to know about all events at respectively $a_1$ and $a_2$, but now also a partial view for their reads from $a_{\text{clock}}$. The partial view ensures that wrapper$^{22}$ does not need to update its view whenever wrapper$^{21}$ reads a timestamp from the clock. vice versa. Iris already contains a monotone resource algebra, that could allow implementing such partial views.

layers this way: the invariant for wrapper $x_1$ in Fig. 16 owns a resource filter_val $\gamma_{pr(x_1)} \, F \, x_1 \, t_{x_1}$, which states that $x_1$’s view on the trace is $t_{x_1}$, and that $t_{x_1}$ is obtained by applying a filter $F \, x_1$ to the view $\text{pr}(x_1)$ that $pr(x_1)$ has. As shown in the bottom of the figure, this resource connects to the resource filter_full $\gamma_{pr(x_1)} \, \text{pr}(x_1)$ in wrapper $pr(x_1)$, which represents the full view. Here, $\gamma_{pr(x)}$ is simply a name used to distinguish different filtering systems. The root wrapper has a view on the entire physical trace, i.e. its invariant owns a resource filter_val $\gamma \, \text{id} \, t$ where $\text{id}$ is the identity filter and $t$ is the physical trace. Note that top-level wrappers do not require a resource filter_full $\gamma \, t$, since they do not provide a view on the trace to a higher-level wrapper. When proving $\text{OBJ-X}$ for a wrapper $x_1$, $x_1$ and its siblings are the top level wrappers.
with the trace, e.g. if a wrapper updates its local state before invoking the layer-below wrapper to perform IO, or if updating the local state takes multiple instructions. For this reason, invPs(x) consists of two parts: an atomic invariant invPs,x, which ensures that the security objective holds continuously, and a so-called non-atomic invariant invst,x, which ensures (among other things) that the local state is satisfied. The resources cur_tr γbxz t_e and cur_tr γbxz t_x in Fig. 16 enforce that the view of the trace in both invariants is the same. Fig. 17 illustrates how both types of invariants are upheld if the local state can temporally be broken while a lower-level wrapper is executing and reestablished afterwards, whereas all atomic invariants have to be updated at the same time, during the instruction that performs the physical MMIO effect.

4) Putting it all together: Given the representation of invPs,x in Fig. 16 we now denote this atomic invariant with all of its parameters as invPs(Fx, Px, tp, γps(x), γbxz, γx). The only new parameter is the boolean tp, which denotes whether x is currently considered a top-level wrapper. This is important to know since, as mentioned, the resource filter_full γx t_x is not present if x is a top-level wrapper. The arguments γps(x), γbxz, γx are omitted if they are clear from context.

To exemplify the previous discussion, we investigate the atomic invariants involved in proving OBJ-21 (the non-atomic invariants are more tedious and less interesting). The invariants are as follows:

\[
\text{invP}(\text{id} \rightarrow \text{False}, \gamma_0, \gamma_{b0}, \gamma_1) \land \text{invP}(\text{id} \rightarrow \text{False}, \gamma_1, \gamma_{bxz}, \gamma_2) \\
\text{invP}(F_{21}, P_{21}, \text{True}, \gamma_{21}, \gamma_{bxz}, \gamma_2) \\
\exists x. \text{filter_val}_2 \gamma_2 F_{21} \gamma_2
\]

The first three invariants represent wrappers 0, 1 and 21. Since wrappers 0 and 1 are the only wrappers in their layer, they apply the identity filter id to the previous layer’s trace. The resource filter_val γ0 id t in wrapper0’s invariant is linked to the actual physical trace. The third invariant, wrapper21’s proper invariant, enforces the first conclusion of OBJ-21 through the presence of F_{21} and P_{21}. Additionally, the fourth invariant ensures that no other addresses than a_1 and a_2 receive MMIO events. From the point of view of the top-level wrapper_21 in Fig. 18, the third layer is irrelevant, so the third invariant has tp set to True, whereas non-top-level wrappers 0 and 1 have it set to False. Also note the _ in place of P_0 and P_1 in the first two invariants, indicating that wrapper_21 does not care what predicate the lower wrappers enforce when proving its own security objective.

B. Functional correctness of wrappers

The invariants discussed in the previous section are used to prove two contracts for every wrapper: a form of functional correctness and a form of security. We will discuss the proofs of security in more detail in the next section, and the proofs of correctness now. The correctness contract expresses that when a wrapper is invoked, it either generates the desired external effect or throws an error in case the effect would violate their policy.

These contracts are expressed in terms of a program logic for our capability machine, which we inherit from Georges et al. [11] and extend with rules for the MMIO cases of the load and store instructions. The program logic contains the following weakest precondition assertion:

\[
\text{wp} \text{ Repeat SingleStep} \{ s, Q(s) \} \\
\text{wp} \text{ Repeat SingleStep} \{ s, \varphi(s) \} \\
\]

In terms of wp \{ \}, we can define a form of contract triple \{ P \} Repeat SingleStep \{ Q \} that we define (roughly) as follows:

\[
\forall \varphi. P \Rightarrow (Q \Rightarrow \text{wp} \text{ Repeat SingleStep} \{ s, \varphi(s) \}) \\
\Rightarrow \text{wp} \text{ Repeat SingleStep} \{ s, \varphi(s) \} \\
\]

In terms of this abstraction, the functional correctness contract of the write closure of a wrapper x could look roughly as follows (omitting error cases and technical details):

\[
\text{filter_val}_x (\lambda t. \text{filter}(P_0, t)) t \mapsto P_0(\text{IOWrite}, a, v) \\
\{ \text{pc} \mapsto (p_w, b_w, e_w, a_w) \} \\
\{ f_0 \mapsto w_{ret} \land f_1 \land v \land f_2 \mapsto a \} \\
\text{Repeat SingleStep} \\
\text{filter_val}_x (\lambda t. \text{filter}(P_e, t)) (t \mapsto [(\text{IOWrite}, a, v)]) \\
\{ \text{pc} \mapsto \text{updatePcPerm}(w_{ret}) \} \\
\{ f_0 \mapsto w_{ret} \land f_1 \land v \land f_2 \mapsto a \} \\
\]

where the updatePcPerm function maps E capabilities to their RX counterparts and leaves other capabilities untouched, and we used the fact that filters in our current examples are event-based (cfr. the definition of validity in Fig. 15) to rewrite Fx as (λt. filter(P_e, t)). This contract expresses that when the write closure is invoked and the pc contains a capability (p_w, b_w, e_w, a_w), with arguments v and a and a return capability

---

2Two caveats: (1) we do not use this abstraction in our Coq development but use the unfolded definition directly and (2) most of our contracts use a variant of this definition that allows the program to fail at an arbitrary point of execution.
unmodiﬁed register contents. Additionally, a filter_val \( \gamma_x \) \((\lambda t. \text{filter}(P_t, t)) t\) resource is required to update the filter_full \( \gamma_x t\) resource in \( \text{inv}_{P,x} \) using property \( 3 \) in Fig. 15. To prove the orthogonality precondition to this property, \( P_t \) needs to accept the requested external effect (IOWrite, \( a, v \)). In the postcondition, an updated filter_val resource is returned to express that the effect has been performed.

Unfortunately, the above contract does not quite work. The problem is that higher-level wrappers who wish to invoke a lower-level write closure do not directly own the necessary resource filter_val \( \gamma_x \) \((\lambda t. \text{filter}(P_t, t)) t\). As we discussed, this resource is embedded in an invariant \( \text{inv}_{P_t} \). Because this invariant is atomic, it must be restored after every individual instruction, as was already illustrated in Fig. 17. It is therefore not possible to extract the resource from the invariant for the duration of the wrapper invocation.

To solve this problem, we employ the technique of Higher-Order Concurrent Abstract Predicates (HOCAP) [19, 20]. The client wrapper will not extract the filter_val \( \gamma_{pr(x)} \) \((\lambda t. \text{filter}(P_t, t)) t\) resource from its invariant and restore it after the invocation. Instead, it delegates the work of updating its invariant to the invoked wrapper, and the invoked wrapper will do this at exactly the right execution step, namely the step that executes the MMIO write. This means the contract will look as follows (again omitting error cases and technical details):

\[
\begin{align*}
&\{ \begin{aligned}
&\forall t. \text{filter}_\text{full} \gamma_x (t * P) \Rightarrow \\
&\text{filter}_\text{full} \gamma_x (t + [(\text{IOWrite}, a, v)]) * Q
\end{aligned} \\
&* P * pc \mapsto (p_w, b_w, e_w, a_w)
\}
\]

Repeat SingleStep

\[
\begin{align*}
&\{ Q * pc \mapsto \text{updatePcPerm}(w_{ret}) \\
&* r_0 \mapsto w_{ret} * r_1 \mapsto v * r_2 \mapsto a
\end{align*}
\]

In this contract, the caller provides a so-called view shift to the wrapper invocation: a type of logical callback that expresses how the lower-level wrapper \( pr(x) \) can update the client wrapper \( x \)'s invariant for them. View shifts are the reason why, in Fig. 17 wrapper0 was capable of immediately reestablishing the atomic invariants of wrapper1 and wrapper2 when it performed MMIO. Note that the client does not need to provide their filter_val \( \gamma_x \) \((\lambda t. \text{filter}(P_t, t)) t\) resource beforehand, but instead is allowed to rely on the invoked wrapper’s filter_full \( \gamma_x t\) resource in the proof of the view shift. In this proof, the view shift is allowed to consume additional client resources \( P \) that the caller has to provide at the start of the invocation, and produces resources \( Q \). Note that, since top level wrappers contain no filter_full \( \gamma_x t\) resource that needs to be updated externally, their contracts need not be parameterized by a view shift. In other words, the same boolean \( tp \) we discussed in the previous section will determine whether a wrapper’s contract is parameterized by a view shift.

\[
\mathcal{E}(v) \triangleq \forall \text{reg}. (\mathcal{R}(\text{reg}) * \text{pc} \mapsto v * \star_{(r,v) \in \text{reg}, r \neq \text{pc}} r \mapsto w) \rightarrow wp \text{ Repeat SingleStep} \{-\top\}
\]

\[
\mathcal{R}(\text{reg}) \triangleq \star_{(r,v) \in \text{reg}, r \neq \text{pc}} \mathcal{V}(v)
\]

\[
\mathcal{V}(v) \triangleq \begin{cases}
\forall \gamma x, \gamma_{pr(x)}, \gamma_{bx}, \gamma_{a} \leftarrow \langle \forall t. \text{filter}_\text{full} \gamma_x t * P \Rightarrow \text{filter}_\text{full} \gamma_x (t + [e]) * Q \rangle \rightarrow \\
\forall t. \text{filter}_\text{full} \gamma_{pr(x)} t * P \Rightarrow \text{filter}_\text{full} \gamma_{bx} (t + [e]) * Q \rightarrow \\
\text{cur}_t \text{tr} \gamma_{bx} t \Rightarrow \text{filter}_\text{full} \gamma_{pr(x)} (t + [e]) * Q \Rightarrow \\
\text{cur}_t \text{tr} \gamma_{bx} (t + [e])
\end{cases}
\]

This theorem states that the view shift is \( x \) parameterized by \( pr(x) \) can be lowered to one that satisfies the contract for \( pr(x) \), if \( x \) can provide the additional guarantee that \( P_t(x) \) and \( P_e(t + [e]) \) hold (which is precisely what \( x \) checks before admitting the event anyway), and if \( x \) makes \( pr(x) \) update the trace in the local state invariant \( \text{inv}_{st} \). Recursively applying this theorem allows efficiently deriving higher-level driver specifications from lower-level ones. Note that view shift lowering accumulates resources in \( P \) and \( Q \) until the bottom-level driver is reached, at which point all higher-level invariants \( \text{inv}_{P,x} \) are updated at once.

C. A semantic model for capability safety

In this section, we describe how we reason about the fact that unknown adversarial code satisfies the security objectives. We use a logical relations model to capture the notion of capability safety, i.e. the universal contract, that the hardware capabilities provide. Concretely, we will verify that our own wrapper closures are safe to execute, and that the adversary’s code is safe to execute, starting from safe register states, in particular states containing the wrappers’ closures.

Since our capability machine builds upon the bare-bones capability machine of Georges et al. [11], we reuse their logical relation without revocation and its formalization in Iris, and repeat a simpliﬁed version of the separation logic deﬁnition in Fig. 18. Additionally, we reprove their fundamental theorem (Theorem 2 below) in the presence of MMIO.

We restrict our explanation of Fig. 18 to the essentials required to understand the key concepts behind our proofs. The model consists of three different, mutually recursive relations:
The value relation $V : \text{Word} \rightarrow \text{iProp}$ (with iProp the type of propositions in Iris) defines when a word is safe.

The expression relation $E : \text{Word} \rightarrow \text{iProp}$ defines when a capability can safely be executed in the pc register.

The register relation $R : \text{Reg} \rightarrow \text{iProp}$ lifts the value relation to an entire register bank (bar the pc). A register bank is safe if each general purpose register is safe.

Technically, these relations are well-defined by so-called guarded recursion, see [11], [21].

We first discuss the definition of the value relation. $V(w)$ specifies an upper bound on the authority over memory that the word $w$ carries. Since integers and o-capabilities do not represent any authority over memory, they are always safe, as expressed by $\top$. Enter capabilities are safe if it is safe to execute them in the pc after jumping to them (hence the RX permission). The presence of the persistent modality $\Box$ and the later modality $\triangleright$ can be ignored by readers unfamiliar with them. All remaining capability types have read permission and these capabilities are safe if, for each $a'$ in their memory range $[b, e)$, an Iris invariant (denoted by a boxed assertion) exists that asserts that memory location $a'$ will always contain a safe value. The assertion $a' \mapsto w$ in the invariant expresses unique ownership of the memory location $a'$ with permission $p'$ and stored word $w$. Additionally, this assertion implies that $a'$ cannot be an MMIO location. This ensures that adversaries cannot gain direct access to MMIO memory and bypass our wrappers. Note that the invariant permits using a $p'$ that is at least as strong as $p$, i.e. $p \preceq p'$. This allows for downgrading of capability permissions and aliasing of different permissions. Notice that no additional assertions have to be added to the definition of $V(p, b, e, a)$ for capabilities that carry additional write or execute authority. The intuitive reason is that the invariant already enforces that any written value needs to be valid, and that having read authority over a part of memory suffices for an adversary to copy code over to a region to which it has write-execute permission over, and execute it there.

Next, we discuss the execution relation $E$. It states that, given ownership of any initial register bank $\text{reg}$ that satisfies the register relation $R$, we can safely run the machine with $v$ in the pc register. The weakest precondition assertion $\text{wp}$ uses a trivial postcondition $\top$, which at first sight might seem odd. This suffices because Iris’ weakest precondition implicitly enforces that all invariants hold at each step of execution. Thus, any invariants related to $\Box$ that a wrapper might define will also be enforced through the expression relation by the $\text{wp}$ assertion. For example, if wrapper$_1$ were to set up an invariant that ensures that $P_1(t)$ holds over the current trace $t$, i.e. $P_1(t)$, then this invariant is upheld at each step of execution when jumping to Adversary 1, under two conditions. First, Adversary 1 should be safe to execute, i.e. $E(\text{RwX}, \text{adv}_{b_1}, \text{adv}_{e_1}, \text{adv}_{b_1})$ holds. Second, to meet the precondition of the expression relation, Set-up Code 1 has to pass the adversary a safe register block, which notably requires proving that the read and write closures for wrapper$_1$ are safe, since they are shown to be located in $t_1$ and $r_2$ when jumping to Adversary 1 in Fig. [10]. This latter condition can be proven relatively straightforwardly from the contracts we described in Section [IV-B]. We hence focus on proving the different adversaries in our examples safe, by leveraging the FTLR (fundamental theorem of the logical relation).

The fundamental theorem has the following simple statement:  

**Theorem 2 (FTLR):** \( \forall w \cdot V(w) \rightarrow E(w) \).

In other words: if a word is safe, it can safely be executed as well. The statement is identical to Georges et al.’s FTLR, but the proof is slightly different due to the presence of MMIO.

Through this theorem, it is easy to prove that for each region Adversary X in Fig. [9], $E(\text{RwX}, \text{adv}_{b_X}, \text{adv}_{e_X}, \text{adv}_{b_X})$ holds. Since each init_config X predicate requires initial memory to not contain any capabilities, since integers are always safe, and since the different set-up codes do not change the adversary’s memory, $V(\text{RwX}, \text{adv}_{b_X}, \text{adv}_{e_X}, \text{adv}_{b_X})$ holds. The fundamental theorem then proves the result.

### D. Sharing verification effort for fixed-structure wrappers

For wrappers $x$ that satisfy some conditions, we have developed a method in Coq that requires minimal manual verification effort in proving the functional contract and safety of the closures for these drivers. The conditions are as follows:

- Respect the calling convention described in Section [III]
- Enforce their security objective using an atomic invariant of the form $\text{inv}_P(F_x, P_x, tp_x)$.
- Consist of a single read and write closure, and only jump to the read and write closures of their layer below driver. The state invariant $\text{inv}_\text{st}$ expresses both ownership of the code for $x$, and describes the closures for $pr(x)$ in the local state, and will hence be parameterized by the relevant addresses of both $x$ and $pr(x)$. It is then denoted as follows: $\text{inv}_\text{st}(d_{pr(x)}, d_{w_{pr(x)}}, d_{e_{pr(x)}}, d_{r_x}, d_{w_x}, d_{e_x})$.
- Have an implementation that satisfies a specific template, which is parameterized by instructions check_read and check_write to check $P_x \circ F_x$ in respectively the read and write closures. Wrapper 1 in Fig. [13] is structured like this, for example.

If these conditions are satisfied, the only manual effort involved is a proof that check_read and check_write indeed correctly enforce $P_x \circ F_x$ on $x$’s view of the trace, denoted by check_spec_read($F_x, F_x$, check_read) and check_spec_write($F_x, P_x$, check_write), respectively. These conditions are enforced in the local state invariant $\text{inv}_\text{st}$, adding the parameters $P_x$ and $F_x$ to it.

Under the above conditions, we can define simple contracts in the style of Section [V-B] for the driver’s read and write closures, that only depend on $d_{r_x}, d_{e_x}, d_{r_x}/d_{w_x}$, and $tp_x$ (to determine whether or not a view shift is required in the contract), and are denoted read_spec($d_{r_x}, d_{e_x}, d_{r_x}, d_{w_x}, tp_x$) and write_spec($d_{r_x}, d_{e_x}, d_{r_x}, d_{w_x}, tp_x$).

We can then state the following lifting theorem:  

**Theorem 3 (Lifting-theorem-read):**  
\[
\begin{align*}
\text{inv}_P(F_x, P_x, tp_x) \\
\text{read_spec}(d_{pr(x)}, d_{e_{pr(x)}}, d_{r_{pr(x)}}, \text{False}) \\
\text{inv}_st(d_{pr(x)}, d_{w_{pr(x)}}, d_{r_{pr(x)}}, d_{e_{pr(x)}}, d_{r_x}, d_{w_x}) \\
\text{read_spec}(d_{r_x}, d_{e_x}, d_{r_x}, tp_x)
\end{align*}
\]
A similar result holds for the write spec. Note that this theorem is generic in $t_{p_x}$. It states that if all necessary conditions on the state of a wrapper are met ($inv_{st}$), and if an invariant enforces $F$ and $P$ on the trace ($inv_{tr}$), then we can lift a spec for the pointed-to wrapper in the previous layer, to the current layer. The bottom-most wrapper, i.e. wrapper$_0$, in the examples, constitutes the base case in this theorem, and still has to be manually verified to satisfy $read_{spec}$ and $write_{spec}$, since its code and local state do not satisfy the template (cfr. Fig. 11 and $LS_0$ in Fig. 7).

Finally, we can prove top-level wrapper closures secure using the following theorem:

**Theorem 4 (Wrapper-safety-read):**

$$read_{spec}(d_{-r_x}, d_{-e_x}, d_{-r_x}, True) \rightarrow V(e, Global, d_{-r_x}, d_{-e_x}, d_{-r_x})$$

Again, a similar result holds for the write spec.

Since we have abstracted most reasoning related to wrappers into Theorems 3 and 4, the check_read and check_write instructions are indeed the only code we need to hand-verify to ensure wrapper safety. We used this approach to verify the first example. The shape of the local state and the code of the second example is slightly different, due to the presence of the timer closure, so it did not fit this approach. However, Theorem 4 still applied once the $read_{spec}$ and $write_{spec}$ were proven.

V. RELATED WORK

Hardware-supported security mechanisms as well as software verification have been important ingredients of secure system development for a long time [22]. We discuss the most important lines of related work and how they differ from our results.

One distinguishing feature of our work is that we support robust modular verification. Robust verification requires underlying programming language or hardware support to protect verified code from untrusted code. Earlier work has demonstrated how to robustly verify safety properties in settings where that protection is not needed. For instance, Sammler et al. [23] and Jia et al. [24] have proposed approaches to robustly verify safety properties in the presence of untrusted code that is confined using some sandboxing mechanism. Alternatively, Agen et al. [25] have used trusted execution environments (TEEs) like Intel SGX [26] or Sancus [27] to protect a verified module from an unverified context, but verification is at the level of C code and their focus is on proving assertions about the protected module rather than full system properties. In our approach, protection of verified code is provided by the capability-based instruction set architecture, and this enables handling of nested protection.

Protecting verified code from unverified code is of course closely related to protecting trusted system software from untrusted user code. Operating systems, microkernels, and hypervisors use hardware privilege levels to protect themselves, and hence the rich line of work on verifying properties of such system-level software can be seen as an instance of robust modular verification and hence related to our work. Some important milestones include the verification of the seL4 microkernel [28], [29], and the verification of Microsoft’s Hyper-V hypervisor [30]. The focus is however on proving properties (such as functional correctness, or selected safety properties) of the system software under a single attacker model where all non-privileged code is trusted. Like our work, the verification of CertiKOS [31] supports modular (compositional) and layered verification of device drivers. But an important difference is that verification in CertiKOS is compositional but not robustly modular: only user-level code is isolated at run time from kernel-level code, and any unverified code at kernel-level becomes part of the trusted computing base. The journal version of the CertiKOS driver verification paper [32] also has an extensive overview of other related work on operating system verification.

The usefulness of being able to nest protection systems has been recognized in the system security research community, and several systems have been proposed that support, for instance, nested virtualization [33], [34]. However, for none of these systems, any code-level formal guarantees are provided.

It is the reliance on capabilities as the underlying protection mechanism that enables arbitrary nesting for our approach. Capability-based architectures have a rich history [4], and have been proposed as a security foundation for both high-level languages [35], [12], [8] and assembly languages [5]. The fact that capabilities support nesting has been observed before, e.g. in Mark Miller’s PhD thesis [46]. It has also been known for a long time that they provide a great foundation for nestable security architectures in high-level languages [37]. Over the past decade, capabilities at the instruction set architecture level have seen renewed interest, largely thanks to the CHERI project [6]. CHERI is a hybrid architecture that supports capability-based protection for user-level code and classical memory protection for isolating kernel and processes. Hence, CHERI does not use the nested encapsulation for wrappers that we study in this paper. However, CheriRTOS [38], a CHERI-aware real-time operating system, supports capability-based fine-grained isolation for device drivers and would be a candidate implementation platform for our verified wrapper stacks.

Capability-based systems support the enforcement of security properties in the presence of arbitrary untrusted code in the system through what are typically called object capability patterns, like the membrane or caretaker patterns [36]. It is only relatively recently that sufficiently powerful formal reasoning approaches have been developed that can prove such properties. Devriese et al. [7] proposed a reasoning approach based on logical relations, (what we now call) universal contracts and the concept of effect parametricity. Swasey et al. [8] developed the first program logic, OCPL, that can compositionally specify and verify the properties enforced by object capability patterns. Building on these ideas, program logics have been developed to reason about software in low-level capability-based instruction set architectures [10], [11]. These logics, as ours, are built in Iris [21], a separation logic framework for building program logics. Iris integrates, unifies, and simplifies a wide variety of mechanisms for reasoning about programs that can be higher-order, concurrent, or use mutable state. The results in this paper
can be seen as an application and extension of these logics to prove security properties for multiple stakeholders in a system with nested encapsulation.

One of the motivations for our approach is the minimization of the Trusted Computing Base (TCB). The various stakeholders in the system want to ensure their security objectives while trusting as little other software as possible. The use of small software modules isolated by some hardware protection mechanism to enforce full-system security properties has been proposed in multiple guises in the system security field. DriverGuard [39] uses virtualization techniques to implement fine-grained protection on I/O through specific devices with a small TCB. Para-passthrough virtualization [14] specifically aims to provide full-system guarantees while relying only on a small piece of software, albeit for only a single attacker model. One could argue that micro-kernels or hypervisor-based systems are similar. We show that it is possible to apply this principle at multiple levels in the same system and verify security.

Related to minimization of the TCB is the idea of compartmentalization, breaking a large program in smaller mutually distrustful parts and relying on some underlying security mechanism to protect the parts from one another. Juglaret et al. [40] have studied the formal guarantees provided by a compartmentalizing compiler. They consider multiple compromise scenarios, where an attacker can compromise different subsets of program parts, somewhat similar to our consideration of multiple attacker models. However, they only consider the benefits provided by a compartmentalizing compiler, and do not consider verification.

If the full system security objectives to be verified include statements about I/O through a given device, then necessarily the device driver(s) for that device will need to be verified. Hence, the approach proposed in this paper verifies a subset of the driver stack for a device depending on the attacker model. Device drivers have been a target of verification in a wide body of related work, using techniques ranging from model checking (e.g. [41]) to deductive verification (e.g. [42]). The objective of these verification efforts is to improve kernel reliability by showing that drivers correctly use specific kernel APIs, or do not have memory safety or concurrency bugs. That is very different from our objective of verifying that a thin wrapper around a device enforces a specified security property.

VI. CONCLUSION AND FUTURE WORK

The fine-grainedness of hardware capabilities, in combination with object capabilities as a primitive enabling encapsulation, allows for efficient and safe nesting of wrappers enforcing security properties without costly context switches. This would be hard to achieve through conventional, more coarse-grained security primitives. By capitalizing on capabilities and extending an existing formal model for a capability machine, we managed to generalize classical robust modular verification to a nested setting. With nested robust modular verification, a system that consists of multiple layers is verified robustly several times, each time verifying an increasing number of layers and enforcing more security objectives, and considering the rest of the code base as well as the environment untrusted. Crucially, our approach retains the compositionality of the programming logic and does not require verifying the same code multiple times, even when proving security objectives for different layers. Our Iris development provides ease of use when modularly verifying nested wrappers, only requiring specific checking instructions to be verified and lower layer wrappers proven safe, in order to obtain proofs of safety for an entire stack of wrappers. These proofs of wrapper safety are essential in proving the different full-system security properties.

In future work, we wish to extend our basic model of IO, to achieve nested full-system guarantees in more involved settings. Concretely, we believe it to be possible to achieve similar guarantees when adding interrupts to the basic capability machine. This would require formalizing interrupts dynamics, redefining the notion of weakest precondition correspondingly, as well as proving specifications for registered interrupt handlers themselves. Another interesting extension is allowing peripherals to perform some form of capability-restricted DMA access, as hinted at by Markettos et al. [43]. Additionally, with the advent of modern capability hardware in the form of Arm’s Morello prototype [44], it will soon become possible to perform practical experiments on capability-enabled hardware, thereby obtaining a fair comparison between our work and similar approaches using different security primitives.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for valuable comments and suggestions. This work was supported in part by a Villum Investigator grant (no. 25804), Center for Basic Research in Program Verification (CPV), from the VILLUM Foundation; by the Research Foundation - Flanders (FWO); and by DFF project 6108-00363 from The Danish Council for Independent Research for the Natural Sciences (FNU). This research was partially funded by the Research Fund KU Leuven, and by the Flemish Research Programme Cybersecurity. Thomas Van Strydonck holds a Research Fellowship of the Research Foundation - Flanders (FWO). Amin Timany was a postdoctoral fellow of the Flemish research fund (FWO) during parts of this project.

REFERENCES


