HLIO: Mixing Static and Dynamic Typing for Information-Flow Control in Haskell

Pablo Buiras
Chalmers University of Technology, Sweden
buiras@chalmers.se

Dimitrios Vytiniotis
Microsoft Research, United Kingdom
dimitris@microsoft.com

Alejandro Russo*
Chalmers University of Technology, Sweden
russo@chalmers.se

Abstract
Information-Flow Control (IFC) is a well-established approach for allowing untrusted code to manipulate sensitive data without disclosing it. IFC is typically enforced via type systems and static analyses or via dynamic execution monitors. The LIO Haskell library, originating in operating systems research, implements a purely dynamic monitor of the sensitivity level of a computation, particularly suitable when data sensitivity levels are only known at runtime. In this paper, we show how to give programmers the flexibility of deferring IFC checks to runtime (as in LIO), while also providing static guarantees—and the absence of runtime checks—for parts of their programs that can be statically verified (unlike LIO). We present the design and implementation of our approach, HLIO (Hybrid LIO), as an embedding in Haskell that uses a novel technique for deferring IFC checks based on singleton types and constraint polymorphism. We formalize HLIO, prove non-interference, and show how interesting IFC examples can be programmed. Although our motivation is IFC, our technique for deferring constraints goes well beyond and offers a methodology for programmer-controlled hybrid type checking in Haskell.

Categories and Subject Descriptors D.1.1 [Programming Techniques]: Applicative (Functional) Programming; D.3.3 [Programming Languages]: Language Constructs and Features; D.4.6 [Security and Protection]: Information flow controls

Keywords Information-flow control, hybrid typing, gradual typing, dynamic typing, data kinds, constraint kinds, singleton types

1. Introduction
Preserving confidentiality of data has become of extreme importance, particularly in complex systems where untrusted components require access to sensitive information (e.g., text messages, contact lists, pictures, etc.) in order to provide their functionality. Information-Flow Control (IFC) is a well-established approach for allowing untrusted code to manipulate sensitive data without disclosing it (Sabelfeld and Myers 2003). IFC essentially scrutinizes source code to track how data of different sensitivity levels flows within a program, where security alarms are raised when confidentiality might be at stake. IFC research has produced three mature compilers for secure programs: Jif (Myers and Liskov 2000) (based on Java), FlowCaml (Simonet 2003) (based on Caml and not developed any more), and Paragon (Broberg et al. 2013) (based on Java). Alternatively, IFC can be provided via simple libraries in Haskell where concepts like arrows and monads are repurposed to protect confidentiality (Li and Zdancewic 2006; Russo et al. 2008).

There exists a broad spectrum of enforcement mechanisms for IFC, ranging from fully dynamic ones, e.g., in the form of execution monitors (Austin and Flanagan 2009; Askarov and Sabelfeld 2009), to static ones, e.g., in the form of type systems (Volpano et al. 1996). Although dynamic and static techniques provide similar security guarantees (Sabelfeld and Russo 2009), there are many arguments for choosing dynamic over static approaches and vice versa. Several of these arguments have their roots in the long-term dispute between dynamic and static analyses, e.g., overhead vs. performance, enforcing properties for a program once and for all vs. monitoring properties in every run of a program, etc.

From the security point of view, specifically, there are good reasons to prefer dynamic over static approaches. Code statically verified to preserve confidentiality clearly adheres to data sensitivity levels and policies valid at compile time. However, data sensitivity levels may be entirely dynamic (e.g., we may read data from a trusted or a non-trusted domain at runtime) and even policies may change at runtime (e.g., principals can change the set of principals they share data with by—for instance—altering their list of friends). In situations like this, the statically verified code has to be restructured to perform runtime checks in ways that the static analysis or the type system can understand and exploit to verify the program (we will see an example of that in Section 3). Alternatively, programs have to be written in a way that can statically deal with all possible sensitivity levels or policies that they could potentially encounter at runtime; this in turn may limit the set of useful side-effects programs can perform.

The LIO library (Stefan et al. 2011b) for Haskell offers a way of tackling this problem by providing a monad that dynamically enforces IFC. Borrowing ideas from operating systems research (VanDeBogart et al. 2007; Zeldovich et al. 2006), the LIO monad implements an execution monitor that keeps track of a current label to indicate the sensitivity level of the computation. The current label may get raised, or tainted, when the computation depends on sensitive data. Furthermore, sensitive computations are prevented from writing into public channels. In practice, LIO has proven suitable for building production secure web systems (Griffin et al. 2012).

There are plenty of opportunities to optimize away LIO runtime security checks. For example, it is enough to perform a single check...
for computations that, within a long loop, attempt to write to the same channel without affecting the current label. Ideally, runtime checks should only be applied to those parts of the program where sensitive labels are unknown at compile time or susceptible to changes at runtime. Although a state-of-the-art tool, LIO does not support mixing static and dynamic IFC. In this work, we address this shortcoming.

We present HLIO, a Hybrid IFC library which combines the best of both approaches. HLIO statically protects confidentiality while allowing the programmers to defer selected checks to be done at runtime. In that manner, security checks involving statically-unknown or prone-to-change labels can be performed at runtime, while providing static guarantees for the rest of the code. Existing LIO code can easily be embedded in HLIO. Furthermore, HLIO provides a very similar interface to LIO. As a result, existing LIO code can also be incrementally refactored to work in HLIO so that programmers can obtain static guarantees where possible.

Our contributions with this paper are:

- We design and implement HLIO, a hybrid approach to IFC that allows programmers to defer IFC constraints to runtime. (Section 4)

- We present a novel technique for embedding HLIO as a library in Haskell. Our technique makes essential use of advanced features of the GHC type system and type inference, namely (a) singleton types (Eisenberg and Weirich 2012), (b) data promotion (Yorgey et al. 2012), and (c) constraint polymorphism\(^1\), i.e., data types that can be parameterized over type class constraints, to enable deferring IFC checks to runtime. We remark that it is not necessary to understand these advanced type system features in order to use our library. (Sections 5 and 6)

- We formalize the core features of HLIO in a calculus that allows us to establish a simulation with LIO, thereby showing that HLIO cannot leak secrets, i.e., that it satisfies termination-insensitive noninterference. (Section 7)

- As an overall contribution, we describe a general-purpose mechanism for deferring static constraints without any compiler or language modifications. Those constraints can go well beyond IFC, and can even include ordinary type equalities emitted by GHC’s type inference engine (see Section 8). We thus make it easier for programmers to move across the static/dynamic boundary, following the mantra of Meijer and Drayton “Static typing where possible, dynamic typing when needed!” (Meijer and Drayton 2005).

2. LIO: Flexible Dynamic IFC for Haskell

In this section, we briefly review LIO and its mechanism for dynamically protecting confidentiality of data.

**Security Lattices** In an IFC system, data gets classified according to its sensitivity degree, which is often denoted by a security label (from now on, just labels). Formally, labels form a lattice \( \text{Label} \) to indicate the allowed flows of information within a program. Data associated with label \( \ell \) can flow into entities labeled as \( \ell_2 \) provided that they respect the order relationship of the lattice, i.e., \( \ell_1 \sqsubseteq \ell_2 \). The encoding of security lattices can be given as a type class, providing join (\( \sqcup \)) and the order relationship (\( \sqsubseteq \))—see Figure 1. In LIO, this type class also includes a meet (\( \sqcap \)) operation, but we exclude it from our definition since it is not important for our purposes.\(^2\) Our running example is the classical two-point security lattice, \( \text{Label} \), that introduces labels \( L \) (low) and \( H \) (high) to classify data as public and secret, respectively.

```haskell
data Label = L | H
instance Lattice Label

The \text{Label} lattice implementation is what one expects; public data can flow into secret entities, i.e., \( L \sqsubseteq H \), but not vice versa, i.e., \( H \not\sqsubseteq L \).
```

**The LIO Monad** LIO provides the \text{LIO} monad to guarantee that computations manipulate data according to the security lattice. In (Stefan et al. 2012b), this monad is parametric on the security lattice being considered, but we consider this lattice to be fixed to type \text{Label} to simplify exposition.

It is expected that untrusted code is written using this monad (and not directly in the IO monad) in order to have some guarantees about its behavior—this can be enforced using other mechanisms (Terei et al. 2012). LIO encapsulates IO actions so that they are only executed when confidentiality is not compromised. To achieve that, the monad keeps track of a label \( \ell_{\text{cur}}: \text{Label} \), called the current floating label (or current label for short), which can be retrieved at any time by the function \text{getLabel}. The role of the current label is two-fold. Firstly, it implicitly labels all the data in scope. Secondly, it only allows computations to write to channels that are labeled with \( \ell :: \text{Label} \) such that \( \ell_{\text{cur}} \sqsubseteq \ell \); otherwise, LIO aborts execution. For instance, a computation \( m :: \text{LIO a} \) with \( \ell_{\text{cur}} = H \) indicates that a secret has already been observed by \( m \)—thus, \( m \) cannot subsequently write to public channels.

**LIO computations** have the flexibility to read sensitive data above the current label, but at the cost of raising the current label and thus being more restrictive in subsequent computations. More specifically, when reading data with sensitivity \( \ell :: \text{Label} \), the current label \( \ell_{\text{cur}} \) is raised to \( \ell_{\text{cur}} = \ell_{\text{cur}} \sqcup \ell \)—in the LIO terminology, the new current label \text{floats above the observed data}. Consequently, the current label protects all the data that have been observed.

```haskell
data Labeled a  
  labelOf :: Labeled a -> Label  
  unlabel :: Labeled a -> a  

getLabel :: MonadLIO getLabel :: Label -> a  
runLIO :: Label a -> IO a
```

**Figure 2. LIO interface**

\(\text{Labeled Expressions} \) As in many other IFC systems, LIO provides abstractions to label data with different sensitivity degrees in a fine-grained manner—see Figure 3. Data type \text{Labeled a} associates an expression of type \( a \) with a label in \( \text{Label} \). The pure function \text{labelOf} can retrieve the label associated with a labeled expression. The functions \text{label} and \text{unlabel} are used to respectively create and destroy elements of this data type. Term \( \ell \) \text{create} a labeled expression which associates label \( \ell \) with expression \( x \), only if \( \ell_{\text{cur}} \not\sqsubseteq \ell \). This constraint ensures that LIO computations do not allocate data below

---

\(^1\) GHC 7.8.1 manual, Section 7.12

\(^2\) Meet is normally used for tracking integrity, e.g. for checking that data has not been corrupted by untrusted parties.
the current label, which could potentially be returned and read by lower-labeled computations.

Term unlabel x never fails; it extracts the data inside a labeled expression x but taints (as a side-effect) the current label by joining it (⊔) with the label of the expression. From a security point of view, creating a labeled expression with label ℓ can be regarded as writing into a channel at security level ℓ. Similarly, observing (i.e., unlabeling) a labeled expression is analogous to reading from a channel with the same security label. For simplicity, we only consider labeled expressions in this paper—they are the simplest examples of labeled entities. Nevertheless, LIO does support labeled mutable references (Stefan et al. 2011b), exceptions (Stefan et al. 2012b), and synchronization variables (Stefan et al. 2012a), which could be orthogonally added.

**Example 1. (Tainting ℓ_cur)** An LIO computation only raises its current label when observing (unlabeling) labeled expressions, as the secure string concatenation example below shows:

```haskell
lconcat :: Labeled String -> Labeled String -> LIO String
lconcat lst1 lst2 = do
  ℓ_cur ← ℓ_cur ∪ (labelOf lst1)
  return (mconcat (unlabel lst1) ++ mconcat (unlabel lst2))
```

**Label Creep** Label creep is the problem of raising the current label to a point where computations are no longer capable of performing useful side-effects (Sabelbaid and Myers 2003), i.e., the current label becomes “too high, too soon.” To address this problem, LIO provides the primitive toLabeled (Figure 3) to allow computations to only temporarily raise their current label. Specifically, toLabeled ℓ m executes m with the current label ℓ_cur at the time of executing this action. It first ensures that ℓ_cur ⊑ ℓ since it would attach ℓ to the result of m—after all, it is creating a labeled value. Computation m can in turn raise the current label during its execution, to a new ℓ_cur. After m terminates, toLabeled checks that ℓ_cur ⊑ ℓ, and if that is the case, label ℓ is used to protect the sensitivity of the result (in the return value of type Labeled a).

In toLabeled ℓ m, ℓ is an upper bound on the final current label of m. The reason for that is to avoid leaks by manipulating the current label inside m (Stefan et al. 2011b). Imagine that the labeled value is instead wrapped with the final current label of m, and that the current label before executing toLabeled is set to L. It could happen that in one run, the current label in m is ℓ₁, where L ⊑ ℓ₁, and depending on information at that level, it decides to unlabel a piece of data which takes the current label to ℓ₂ (ℓ₂ ≠ ℓ₁). After toLabeled gets executed, the next instruction simply reads the label of the returned value (labelOf), which returns either ℓ₁ or ℓ₂ without raising the current label. In that manner, code with current label L can learn from data at level ℓ₁—an information leak!

**Example 2. (Avoiding label creep)** With toLabeled in place, we can provide a more flexible version of lconcat as follows.

```haskell
lconcat' :: Labeled String -> Labeled String
          -> LIO (Labeled String)
lconcat' lst1 lst2 = do
  ℓ_cur ← ℓ_cur ∪ (labelOf lst1) ∪ (labelOf lst2)
  lab ← labelOf lst1 ∪ (labelOf lst2)
  let result = toLabeled lab (lconcat lst1 lst2)
  return result
```

Observe that lconcat’, in contrast with lconcat, can concatenate secret strings without raising the current label.

**Running LIO Actions without Leaking Secrets** Function runLIO uses its first argument to initialize the current label and executes the LIO action given as its second argument. It returns an IO action which is IFC-compliant, i.e., where side-effects do not leak sensitive information with respect to that label.

**Example 3. (Preventing secret leaking)** We describe below a function which runs untrusted code and publishes a returned string value in a public web site.

```haskell
publish :: LIO String -> IO String
publish m = do
  ℓ ← m
  lstr ℓ x ← label L x -- succeeds if ℓ_cur ⊑ L
  unlabel ℓx ← ℓ_cur is not modified
  report s ← wget ("http://reports/str=" ++ s)  ||
```

Function wget sends an HTTP request to the URL given as argument. The action computation runs the untrusted code m but guards the result x with L by calling label L. This call only succeeds when the final label of m is less than or equal to L.

**Dynamically Labeled Values** As mentioned in the introduction, runtime IFC enforcement is particularly useful in systems where values get classified based on runtime information. For instance one can assume (or implement) a primitive that reads a remote labeled value from the network:

```haskell
readRemote :: URI -> LIO (Labeled String)
```

The primitive does not necessarily increase the current label as sensitive data can be encapsulated in the labeled value we return. A more realistic example of such a primitive can be found in the extended version of the paper (Buiras et al. 2015).

Untrusted scripts can freely call readRemote without compromising confidentiality since, in order to observe the returned value, they would have to have their current label tainted and thus would be restricted from performing unsafe side-effects. While not a problem for dynamic LIO, we will see in the next section how dynamically labeled data complicates the programming model in a statically-typed IFC discipline.

3. **SLIO: Static IFC for Haskell**

LIO performs information-flow checks at runtime, and hence the ability to discharge those statically is certainly appealing.

**Security Labels at the Type Level** The first step towards a statically typed version of LIO in Haskell is to transport labels and lattice operations over labels to the type level. We illustrate how this can be done in Haskell for the familiar 2-point lattice:

```haskell
data Label = L | H
```

```haskell
class Flows (ℓ₁ :: Label) (ℓ₂ :: Label)
instance Flows L L
instance Flows L H
instance Flows H H
```

```haskell
type family Join (ℓ₁ :: Label) (ℓ₂ :: Label) :: Label where
  Join L L = L
  Join L H = H
  Join H L = H
  Join H H = H
```

The Label datatype constructors will be used at the type-level. In Haskell terminology, Label will be a promoted datatype (Yorgey et al. 2012). Moreover, we can represent ⊑-constraints at the type level using the type class Flows (ℓ₁ :: Label) (ℓ₂ :: Label) over labels. The instances of the type class encode specific cases of the
Ordinary term-level labels can now be indexed by type-level labels, i.e., they can be defined as singleton types in the dependent type theory jargon—see Figure 4. In a properly typed language, such as Agda or F*, there would be no need for duplication of labels and lattice functionality at the type level and, in fact, our formal treatment (Section 7) does away with the duplication.

Although our running example is the 2-point lattice, we have successfully applied similar techniques to implement a more complicated type-level lattice, namely DC-labels (Stefan et al. 2011a), a decentralized security label model for IFC that can express security concerns from different actors in a mutual distrust environment. As far as we know, this is the first implementation of DC-labels at the type level.

An LIO Hoare State Monad Once the type-level machinery is in place, we replace our dynamic LIO monad with a Hoare state monad (Nanevski et al. 2006), indexed by the initial label of a computation (analogous to a pre-condition) and the final label of a computation (analogous to a post-condition):

\[
data SLIO \ell i :: Label \ell \ell o :: Label \ell a \
runSLIO :: SLIO \ell i \ell o \rightarrow \ell \rightarrow IO a
\]

SLIO is just an intermediate step towards our final solution, but readers can assume a very similar implementation as that of LIO: a state monad over the current label.

\[
type SLIO \ell i \ell o a = SLLabel \ell i \rightarrow \ell \rightarrow (a, SLLabel \ell o)
\]

Due to its more expressive type, SLIO is not a Haskell monad. Nevertheless, it is a monad in the sense that it is possible to define meaningful (\[\Rightarrow\]) and return operators that satisfy the usual monad laws:

\[
(\lambda x . \ell f) \ell a \ell b \ell c \rightarrow (a \rightarrow \ell f \ell b \ell c) \rightarrow \ell f \ell \ell b \ell c \rightarrow \ell \rightarrow \ell \ell \ell
\]

It is easy to see how these functions are implemented.

A Statically Typed API for IFC SLIO so far seems like a more precise typing of LIO. However, the ability to express labels and their operations at the type level immediately opens up the possibility for converting the dynamic checks of LIO to static proof requirements. We do this below by simply rewriting the dynamic API to use static constraints instead:

\[
data Labeled \ell :: Label \ell a = Labeled (SLLabel \ell) a
\]

\[
getLabel :: SLIO \ell i \ell (SLLabel \ell)
\]

\[
labelOf :: Labeled \ell :: Label \ell a \rightarrow SLLabel \ell
\]

\[
label :: Flows \ell i \ell \rightarrow SLLabel \ell
\]

\[
unlabel :: Labeled \ell a \rightarrow SLIO \ell i (\ell (SLLabel \ell) a)
\]

\[
toLabeled :: SLIO \ell i \ell o a \rightarrow SLIO \ell i \ell (Labeled \ell o a)
\]

Function getLabel returns the current label without affecting it. Function labelOf returns the singleton type corresponding to the initial label of the computation. Function label creates a labeled value with label \(\ell\) without modifying the current label \(\ell\), provided that \(\ell' \subseteq \ell\), expressed this time as a static proof obligation.

\[\text{Figure 4. Singleton labels}
\]

Flows \(\ell, \ell\). Function unlabel, on the other hand, taints the current label with the value of the labeled expression. Function toLabeled has a very simple type: just encapsulate the output label in the labeled value that we return. The careful reader may observe a small disconnect between the static and dynamic versions of toLabeled—this is due to a significant simplification that the static world enables, a point we discuss in detail in Section 8.

Finally, in order to give a valid type to primitives such as readRemote, it is often convenient to hide the label of a labeled value with an existential type, so that it no longer appears in the type. Haskell does not support first-class existential types, so we encode this with a datatype definition:

\[
data LabeledX a where
\]

\[\text{Figure 5. Static lReport2}
\]

Problems When Programming in SLIO Let us consider how one can program using the SLIO primitives. Suppose that we have a function report with type

\[
\text{report} :: Flows \ell i \ell L \Rightarrow String \rightarrow SLIO \ell i \ell1 \ell i \ell1\ell i \ell1
\]

that sends a given String to a public server and publishes it on the Internet. This function has a Flows type class constraint which specifies that the current label at the time when report is run should not exceed \(L\), i.e., the public label. For the simple lattice that we consider in this paper, report can effectively be called only when \(\ell i = L\). One could imagine more complex situations with a richer label hierarchy, where more than one label is allowed to report or when the label associated with the public server is not fixed to \(L\) in advance but is rather dynamically obtained. Such situations would amplify our arguments in the rest of this section, but the simpler report above is sufficient for our presentation.

Figure 5 considers the secure string concatenation example concat (from the previous section), except that we instead use the statically typed counterparts to the LIO operations, and we incorporate a call to report in order to publish the result of the concatenation. This function, called lReport2, is a perfectly well-typed program with type

\[
lReport2 :: Flows (Join (Join \ell i \ell1 \ell 2) \ell2) L \Rightarrow
Labeled \ell1 String \rightarrow Labeled \ell2 String
\rightarrow SLIO \ell i (\ell (Join \ell i \ell1 \ell 2) \ell 2) String
\]

Client scripts can call lReport2 provided that they can satisfy the constraint, which enforces that both strings should be public, i.e., labeled with \(L\). For instance, assume that we have \(lv1 :: Labeled L String\), \(lv2 :: Labeled L String\), and code

\[
\text{foo} :: SLIO L L String
\]

\[
\text{foo} = \text{lReport2 lv1 lv2}
\]

All labels are statically resolved, and foo can typecheck as all constraints can be discharged by the type class and type family instances.

Consider now the case where some of the labeled values are dynamically loaded from the network with readRemote from the previous section, and we furthermore address the label creep issue by packing the result in a labeled value:
readRemote :: URI → SLIO ℓ₁ ℓ₂ (LabeledX String)

foo = do
    LabeledX (lv₁ :: Labeled ℓ₁ String) ← readRemote host₁
    LabeledX (lv₂ :: Labeled ℓ₂ String) ← readRemote host₂
    toLabeled (IReport2 lv₁ lv₂)

    The program is ill-typed for two reasons.
    First, the existential label variables ℓ₁ and ℓ₂, arising from unpacking the existential data that we read with readRemote, escape in the return type, i.e., Labeled (Join (Join ℓ₁ ℓ₁) ℓ₂) String. To address this problem we could pack the return type in an existential (using LabeledX) to prevent the existential label from escaping. The modification is shown in Figure 6. However, even if we prevent the escape of existential variables in the return type of foo, there is another problem: the existential variables also escape in the constraints, i.e., Flows (Join (Join ℓ₁ ℓ₁) ℓ₂) L, which makes foo ill-typed.

    Since we do not statically know the remote labels, one may wonder if there is a way to rewrite the program to “assume the worst” (that they are both H) and that the current label after unlabelling them is always—conservatively—H. This option is a non-starter: first, IReport2 would always be returning high-labeled values, but much more worryingly, we would not be in a position to call report any more, even in the case where the actually read remote labels were both L.

    A more appealing way to implement foo is to structure the code to incorporate a runtime test that inspects the remote labels:

    foo = do
        LabeledX lv₁ ← readRemote host₁
        LabeledX lv₂ ← readRemote host₂
        case labelOf lv₁, labelOf lv₂ of
            (1, L) → do
                lv ← toLabeled (IReport2 lv₁ lv₂) :: SLIO ℓ₁ ℓ₂ String
                return (LabeledX lv)
            _ → error "Both strings should be public!"

    The GADT branch on the labels tests for a specific combination of remote labels, which allows the type checker to refine the corresponding type-level labels and discharge all generated constraints. We have also introduced annotations in each branch to fix the SLIO pre- and post-conditions and guide the type inference engine. In the case of the 2-point lattice, the above restructuring is not terrible (only one combination of 4 is a non-error), but more complicated lattices can quickly introduce lots of GADT pattern matches in potentially multiple places inside the user code.

    The example illustrates one awkward aspect of the static approach: every time we have to move dynamic data into a statically typed piece of code, programs have to be restructured to introduce runtime tests. While the runtime tests in this situation are unavoidable, in this paper we show how to do this without restructuring the implementation.

4. HLIO: Mixing Static and Dynamic Typing

In HLIO, users can instead take the “natural” way to write foo and make the program typeable by using our primitive defer (underlined below):⁴

foo host₁ host₂ = do
    LabeledX lv₁ ← readRemote host₁
    LabeledX lv₂ ← readRemote host₂
    lv ← defer (toLabeled (IReport2 lv₁ lv₂))
    return (LabeledX lv)

The role of defer is to defer static constraints to runtime; in this case, the one which arises from toLabeled (IReport2 lv₁ lv₂). This constraint will be ℓ₁ ⊔ ℓ₁ ⊔ ℓ₂ ⊆ L, where ℓ₁ is the initial label and ℓ₁ and ℓ₂ are the labels of the returned labeled values from the two readRemote calls.

To demonstrate how this works, assume that readRemote returns a high-labeled value from host "secure.org", but a low-labeled value from "public.org". The following sequence of calls (using runHLIO, the HLIO analogue of runSLIO) shows that indeed our primitive performs the check at runtime:

ghci> runHLIO L (foo "secure.org" "public.org")
*** Exception: IFC violation!
ghci> runHLIO L (foo "public.org" "public.org")
Success
ghci> runHLIO H (foo "public.org" "public.org")
*** Exception: IFC violation!

In the first case, the first labeled value will contain a high label that taints the current label and results eventually in an IFC exception. In the second case, we only readRemote from public domains and hence no exception is thrown. In the final case, although we read from two public sites, we start from an already high label.

The defer primitive can be used at every point in the assembly of a computation to selectively defer to runtime the constraints arising from a subcomputation, at the programmer’s will. For example, the following variations are all well-typed:

l₁L :: Labeled L String -- a statically known public value
bar x = do
    LabeledX l₁ ← readRemote host₁
    s₁ ← defer (toLabeled (IReport2 x l₁))
    s₂ ← IReport2 x l₁
    return s₂
baz x = do
    LabeledX l₁ ← readRemote host₁
    s₁ ← defer (toLabeled (IReport2 x l₁))
    s₂ ← defer (IReport2 x l₁)
    return s₂

The difference between bar and baz lies in the set of constraints they dynamically check; in bar, we have to statically discharge the constraints that arise from the computation of s₁, but we will dynamically check the constraints arising from IReport2 x l₁ when computing s₁. In baz, we will convert the constraints from s₁ to runtime checks. In both cases, we must defer the constraints that arise from the computation of s₁ as the label of l₁ would otherwise escape in the returned constraint.

The mechanism of defer has also the benefit of addressing the incompleteness of type inference engines or type-level lattice specifications—any time we are faced with a constraint that we cannot statically discharge, defer will convert it to a runtime check.

Having described the functionality we are aiming for, we now present the HLIO API without yet diving into the internals of its implementation.

Label Expressions Whenever a getLabel operation runs, we must produce a runtime representation of the current label, i.e., a singleton. Consider the case where the current label is of the form Join ℓ₁ ℓ₂. When ℓ₁ and ℓ₂ are known statically, we can just apply the type family and compute the resulting label. However, if ℓ₁ and ℓ₂ are existentially quantified, we need a way of computing a single-

---

⁴ We do not yet give type signatures since types slightly differ from the types of the corresponding primitives in SLIO.
ton for the Join by combining the singletons for \( \ell_1 \) and \( \ell_2 \). Therefore, it will be convenient to introduce another promoted datatype that captures unevaluated label expressions as well as a type family to reduce them to Label types. As we will see in Section 6, this additional level of indirection allows us to compute singletons for Join and also to defer constraints involving existentials.

\[ \text{data } LExpr a = LVal a \mid LJoin (LExpr a) (LExpr a) \]

\[ \text{type family } E (\ell :: LExpr \text{ Label}) :: \text{ Label where} \]
\[ E (LVal x) = x \]
\[ E (LJoin \ell_1 \ell_2) = \text{Join } (E \ell_1) (E \ell_2) \]

\[ \text{class Flows } (E \ell_1) (E \ell_2) \Rightarrow \text{ FlowsE } (\ell_1 :: LExpr \text{ Label}) (\ell_2 :: LExpr \text{ Label}) \]

\[ \text{instance Flows } (E \ell_1) (E \ell_2) \Rightarrow \text{ FlowsE } \ell_1 \ell_2 \]

\[ \text{data Labeled } (\ell :: LExpr \text{ Label}) a = \]
\[ \text{Labeled } (\text{SLLabel } (E \ell)) a \]

Data type \( LExpr \text{ Label} \) captures unevaluated label expressions at the type level, and \( E \) reduces them to Label values. The type class FlowsE is isomorphic to Flows, with the exception that it ranges over \( LExpr \text{ Label} \) instead of Label. Note that we also redefine the Labeled data type to include arbitrary labeled expressions. Type family \( LJoin \) encodes \( \sqcup \) at the level of types.

HLIO Monad GHC introduces a kind Constraint to classify constraints and allows constraint polymorphism (Orchard and Schrijvers 2010). This means that ADTs can be parameterized over constraints. HLIO exploits this feature to provide a monad HLIO below:

\[ \text{data } HLIO (c :: \text{ Constraint}) \]
\[ (\ell_1 :: LExpr \text{ Label}) (\ell_2 :: LExpr \text{ Label}) a \]

\[ \text{The } HLIO \text{ datatype is very similar to SLIO except that it also}
\text{records a constraint } c :: \text{ Constraint} \text{ (we motivate this design choice in Section 6). The rest of the HLIO API provides}
\text{mechanisms to discharge these constraints statically or dynamically. A computation } HLIO \ c \ell_1 \ell_2 \ a \text{ should be read as a computation that, under}
\text{constraint } c \text{ and from initial label } \ell_1 \text{ produces a value } a \text{ and raises the current label to } \ell_2. \text{ The types of } (\gg) \text{ and } \text{return} \text{ show how}
\text{constraints are collected:}
\]
\[ (\gg) :: HLIO c_1 \ell_2 \ell_3 \ a \to (a \to HLIO c_2 \ell_3 \ell_3 \ b) \to HLIO (c_1, c_2) \ell_1 \ell_3 \ b \]
\[ \text{return} :: a \to HLIO () \ell_1 \ell_1 \ a \]

Note that the type of \( (\gg) \) creates a tuple of constraints \( (c_1, c_2) \) by collecting constraints \( c_1 \) and \( c_2 \) from the sub-computations. The type of \( \text{return} \) collects a trivial constraint. (1)

IFC Functionality HLIO provides the same API as SLIO:

\[ \text{labelOf } :: \text{ Labeled } \ell a \to \text{ SLLabel } (E \ell) \]
\[ \text{getLabel } :: \text{ HLIO } (\ell \ell_1, \text{ SLLabel } (E \ell_1)) \]
\[ \text{unlabel } :: \text{ Labeled } \ell a \to \text{ HLIO } (\ell \ell_1, (LJoin \ell_1 \ell_1) a) \]
\[ \text{label } :: \text{ SLLabel } \ell a \to \]
\[ \to HLIO (\text{ FlowsE } \ell_1 (LVal \ell)) \ell_1 \ell_1, (\text{ Labeled } (LVal \ell) a) \]
\[ \to \text{ HLIO } c \ell_1 \ell_1, \ell_0, a \to HLIO c \ell_1 \ell_1, \ell_0, (\text{ Labeled } \ell_0 a) \]

Unlike in SLIO, \( \text{label} \) just records constraint \( \text{ FlowsE } \ell_1 \) \( \text{LVal} \ell \) in its result type—instead of actually constraining the whole type of the function. This is the only HLIO primitive that generates a constraint.

Deferring and Simplifying Constraints In addition to the core IFC functionality, HLIO adds the ability to defer collected constraints, or explicitly simplify them in one go:

\[ \text{defer } :: \text{ Deferrable } c \Rightarrow \text{ HLIO } c \ell_1 \ell_0, a \to \text{ HLIO } () \ell_1 \ell_0, a \]
\[ \text{simplify } :: c \Rightarrow \text{ HLIO } c \ell_1 \ell_0, a \to \text{ HLIO } () \ell_1 \ell_0, a \]

The function defer accepts an HLIO computation that would be typeable under constraint \( c \), and returns a computation that is typeable under no constraint! Indeed, the purpose of this combinator is to discharge the constraint by a runtime test. The puzzled reader may wonder how it is even possible to have a sound implementation of defer. The magic is in the Deferrable type class, which we describe in Section 5.

Dually to deferring constraints to runtime, we may require them to be statically discharged—function simplify allows us to do that. Like defer, simplify accepts an HLIO computation that is typeable under constraint \( c \), and returns a computation that is typeable under the empty constraint provided that we can discharge \( c \) statically (hence the quantification \( c \Rightarrow \ldots \)).

Running HLIO Computations Finally, the function that runs HLIO computations is analogous to \( \text{runSLIO} \), except that we require the collected constraints to be provable.\(^5\)

\[ \text{runHLIO } :: c \Rightarrow \text{ SLLabel } \ell \to \text{ HLIO } c \) (LVal \ell) \ell_0, a \Rightarrow \text{ IO } a \]

The Rest of the Paper In the rest of the paper, we describe the Deferrable class which enables us to implement the defer combinator (Section 5), and we present the design decisions and the implementation of the HLIO API (Section 6). We formalize the core features of HLIO as a calculus and prove non-interference by elaboration to (ordinary) LIO (Section 7). We discuss other applications of Deferrable beyond IFC (Section 8).

5 Alternatively, we could equally require that \( c \) be simply Deferrable, or that \( c \equiv () \) and make use of the appropriate defer or simplify combinators when constructing an HLIO computation.
\[ (L, L) \rightarrow L \]
\[ (L, H) \rightarrow H \]

**where** \( p_1 = \bot :: L \Proxy \ell_1 ; p_2 = \bot :: L \Proxy \ell_2 \)

Note that we have given instances for the full range of label expressions \( L \Expr \Label \).

If we have instances for \( T oSLabel \ell_1 \) and \( T oSLabel \ell_2 \) around, then we effectively have runtime witnesses for the corresponding singleton labels, and, in that case, it is very simple to provide an instance for \( \text{Deferrable} \ (F l o w sE \ell_1 \ell_2) \):  

\[
\text{instance} \ (T oSLabel \ell_1, T oSLabel \ell_2) \Rightarrow \\
\text{Deferrable} \ (F l o w sE \ell_1 \ell_2) \text{ where} \\
\text{deferC } p \ m = \text{case} \ (\text{slabel} p_1, \text{slabel} p_2) \ of \\
(L, L) \rightarrow m \\
(L, H) \rightarrow m \\
(H, H) \rightarrow m \\
(H, L) \rightarrow \text{error } \text{"IFC violation!"} \\
\text{where} \ p_1 = \bot :: L \Proxy \ell_1 ; p_2 = \bot :: L \Proxy \ell_2
\]

The implementation of \( \text{deferC} \) pattern matches against the runtime representations of the labels \( \ell_1 \) and \( \ell_2 \). In each corresponding case, the GADT pattern match (e.g. \((L, L)\) in the first case) allows the type system to refine \( \ell_1 \) and \( \ell_2 \) (e.g. \( \ell_1 = LVal L \) and \( \ell_2 = LVal L \) in the first case). Thus, every constraint \( F l o w sE \ell_1 \ell_2 \) required by \( m \) can be refined (e.g. to \( F l o w sE (LVal L) (LVal L) \) in the first case) and can be readily discharged by top-level instances for \( F l o w sE \). It is still possible to forget to include some of the cases, but this will only make the test more conservative.

Note that in the fourth case above (for which no instance exists!), we have no way of calling \( m \), i.e. \( \text{deferC} \) would be ill-typed if we tried. This case corresponds to a genuine runtime error, and we return an error indicating a violation of the IPC policy.

Constraints will be collected together in tuples through uses of \((\Rightarrow)\) and hence we also provide an instance for pairs of constraints, whose definition we omit, i.e., \( \text{Deferrable} (c_1, c_2) \). Finally, we also revisit our definition of \( LabeledX \) to include a dictionary for \( T oSLabel \) to produce a singleton for the existentially-quantified label.

\[
\text{data } LabeledX \ a \ where \ Labeled :: T oSLabel \ell \Rightarrow Labeled \ (\ell :: \Label) \ a \\
\rightarrow LabeledX \ a
\]

This is necessary for applying \( \text{defer} \) to computations involving labeled expressions that have been unpacked from a \( LabeledX \).

The \( \text{Deferrable} \) class is an extremely powerful abstraction for transforming static errors to dynamic checks, and we later show that even type checker equalities generated by the compiler inference mechanism can be deferred (Section 8). We proceed to show how \( \text{Deferrable} \) can be used to implement the \( \text{defer} \) primitive.

### 6. HLIO Design and Implementation

In Haskell, we embed HLIO as a GADT where the constructors correspond to the primitives described in Section 4. More specifically, data type \( \text{HLIO} \) has constructors \( \text{Return}, \text{Bind}, \text{Unlabel}, \text{Label}, \text{ToLabeled}, \text{GetLabel}, \text{Deffer}, \text{and Simplify} \), which represent uninterpreted commands \( \text{return}, \text{bind}, \text{unlabel}, \text{label}, \text{toLabeled}, \text{getLabel}, \text{defer}, \text{and simplify} \), respectively. The types for these constructors match the types given for the commands they represent. In order to give semantics to HLIO terms, we provide an interpretation function \( \text{go} \) with the type

\[
\text{go} :: \forall c \ell \ell_1 \ell_2 \ a. \text{HLIO} \ c \ell \ell_1 \ell_2 \ a \\
\rightarrow (c \Rightarrow \text{SLabel} (\Ell \ell_1) \Rightarrow \text{IO} (a, \text{SLabel} (\Ell \ell_a)))
\]

\[\text{Readers can ignore the proxy arguments } p, p_1 \text{ and } p_2.\]

The interpretation of HLIO is in an IO monad combined with a state to represent the current label (in the style of LIO). Although it might be tempting to get rid of the runtime representation of the current label, this is not possible since code is allowed to inspect it at any time (as a runtime value) using \( \text{getLabel} \).

\[
\text{go} (\text{Return } x) \ell_1 = \text{return} (x, \ell_1) \\
\text{go} (\text{Bind } m \ f) \ell_1 = \text{do } (a, \ell_1) \leftarrow m; \ell_1; \text{go } (f \ a) \ell_1 \\
\text{go} (\text{GetLabel } \ell_1) = \text{return} (\ell_1, \ell_1) \\
\text{go} (\text{Unlabel} (\text{Labeled } v) \ell_1) = \text{return} (v, \ell_1 \ell_1 \text{join} \ell_1) \\
\text{go} (\text{Label } a \ell_1) = \text{return} (\text{Labeled } a \ell_1, \ell_1) \\
\text{go} (\text{ToLabeled} (m :: \text{HLIO} c \ell_1 \ell_2 \ell_3 a')) \ell_1 = \text{do } (x, \ell_1) \leftarrow m; \ell_1; \text{return} (\text{Labeled } a \ell_3 x, \ell_1) \\
\text{go} (\text{Defer } slio) \ell_1 = \text{deferC} \ (\text{setProxy } slio) \ (\text{go } slio \ell_1) \\
\text{where} \ \text{setProxy} :: \text{HLIO} c \ell_1 \ell_2 \ a \rightarrow \text{Proxy } c \\
\text{setProxy} = \text{error } \text{"Proxy!"} \\
\text{go} (\text{Simplify } m) \ell_1 = \text{go } m \ell_1
\]

The interesting cases are the definitions for \( \text{Unlabel}, \text{Deffer}, \text{and Simplify} \). For \( \text{Unlabel} \), \( \text{go} \) performs an ordinary term-level \( \text{join} \):

\[
\text{join} :: \text{SLabel } \ell_1 \rightarrow \text{Label } \ell_2 \rightarrow \text{Label } (\text{Join } \ell_1 \ell_2)
\]

but we never get to inspect the return label unless we explicitly perform a \( \text{getLabel} \) and subsequently strictly use the label, or unless we perform some form of runtime check. For \( \text{Deffer} \), \( \text{go} \) applies the technique from Section 5 with the appropriate proxy. \( \text{Simplify} \) executes \( m \), but exposing its constraints to GHC in order to statically discharge them.

We briefly motivate some of the design choices made in HLIO.

**Singleton Classes** We have seen in the previous section that the motivation for a type-class \( T oSLabel \) containing a singleton \( \text{SLabel } (\Ell \ell) \) comes from the need for deferring \( F l o w sE \) constraints.

**\( LExpr \ Label \) and \( \text{Deferrable} \)** When describing SLIO, we used the \( \text{Label} \) datatype and the \( \text{Flow} \) type class. However, HLIO shifted to datatype \( LExpr \ Label \) and the \( \text{Flow} \) type class to be able to defer constraints. To illustrate the reason behind that, consider an alternative \( \text{Deferrable} \) instance, without all the \( LExpr \) complications, and where \( T oSLabel \) was indexed by \( \text{Label} \):

\[
\text{instance} \ (T oSLabel (\ell_1 :: \text{Label}) \rightarrow T oSLabel (\ell_2 :: \text{Label})) \Rightarrow \\
\text{Deferrable} (\text{Flows } \ell_1 \ell_2) \text{ where}
\]

With this definition, we may find ourselves in need of deferring constraints of the form \( \text{Flows } (\text{Join } \ell_1 \ell_2) \), where \( \text{Join} \) is the \( \ominus \)operation type family implementation directly on \( \text{Labels} \). But type class axioms do not match on type families! (They only match on rigid type constructors.) Consequently, it is impossible to discharge constraint either statically or dynamically. In contrast, by exposing a rigid constructor \( \text{Join} \), we were able to give instances for the join of two labels; with our approach, it is true that the constraint \( T oSLabel (\text{Join } \ell_1 \ell_2) \) is automatically discharged from \( T oSLabel \ell_1 \).

**Embedding Constraints in HLIO** The introduction of constraint \( c \) as part of the HLIO definition achieves a purely syntactic manipulation of constraints, and excludes any possible simplification by GHC—except when the programmer explicitly requires so with \( \text{simplify} \). This aspect is beneficial for two reasons: Firstly, this allows us to prevent eager simplification of certain constraints into a form that cannot be deferred or even discharged. For instance, imagine that a constraint \( \text{Flows} \ell_1 \ell_2 \) floats outside of the HLIO type. In this case, GHC tries to discharge it by proving \( \text{Flows} (\Ell \ell_1) (\Ell \ell_2) \). However, as we discussed before, type class axioms do not match on type families. Moreover, even if
that were possible, deferring such a constraint would require instances of `ToSL` (LValue `ℓ`) and `ToSL` (LValue `ℓ2`), which cannot be constructed from instances of `ToSL` `ℓ1` or `ToSL` `ℓ2`. Secondly, when evaluating a `defer` expression, the constraint `c` in HLIO makes it possible for the `go` function to automatically supply a proxy to instantiate `c` (by unification) for a particular constraint in the type of `deferC`, thus allowing the type checker to select the right instance of `Deferrable` without any help from the programmer. If we were not collecting the constraint `c` in HLIO, the programmer would have to supply these proxies explicitly, making HLIO much more cumbersome to use.

In summary, we have chosen to keep the constraints in their unsimplified form as much as possible, and give the programmer the freedom to decide whether they are to be checked statically or dynamically via explicit annotations (`simplify` and `defer`).

7. Formal Semantics and Non-interference

In this section, we formalize HLIO and provide security guarantees for our approach by interpreting HLIO in LIO and showing an equivalence in the security checks performed by both systems.

Figure 7 presents a type system for HLIO. For the sake of brevity, the figure only shows the security-relevant rules; the remaining rules are standard and can be found in the extended version of this paper. The terms of HLIO are the same as in LIO, with the addition of the `defer` construct. A lattice expression `ℓ` is either a primitive label `Label`, a `join` operation (`⊔`), or a `meet` operation (`⊓`). A constraint `c` is either the empty constraint (⊥), a pair of two constraints ((c, c′)), or a flow constraint among label expressions (ℓ ⊑ ℓ′). The type HLIO is a Hoare state monad in the style of dynamic LIO (Stefan et al. 2012b). Given a well-typed HLIO computation (`interp m`), we provide an interpretation of HLIO in dynamic LIO utilizing LIO primitives. (Function `interp` closely follows the definition of function `go` described in Section 6.)

The function `interp` provides an interpretation of HLIO in dynamic LIO (Stefan et al. 2012b). Given a well-typed HLIO computation `m`, `interp m` runs `m` without performing any security checks, except for those in `deferrable`. This fact can be seen in the deferrable.

---

**Figure 7.** Type system for HLIO.

```
Values

v ::= True | False | () | λx.t | Label

Terms

t ::= v | x | t | fix t | if t then t else t | t ⊗ t | return t | t ⊾ t | getLabel | label t | unlabel t | labelOf t

LVal

Γ ::= Γ1 ⊔ Γ2 | [Γ1]

Lattice

ℓ ::= Label | ℓ ⊓ ℓ | ℓ ⊔ ℓ

Constraints c ::= ((c, c′) | ℓ ⊑ ℓ′)

Types τ ::= Bool | () | τ → τ | HLIO ℓ1 ℓ2 τ

| Label ℓ | Label τ | Label ℓ

RETURN

Γ ⊢ x : τ

BIND

Γ ⊢ m : HLIO ℓ1 ℓ2 a

Γ ⊢ f : a → HLIO ℓ ′ ℓ ′′ b

Γ ⊢ m ≫ f : HLIO (c, c′) ℓ1 ℓ2 b

LABEL

Γ ⊢ t : a

Γ ⊢ s : Label ℓ

Γ ⊢ label s t : HLIO (ℓ1 ⊔ ℓ) ℓ1 (Labeled ℓ a)

UNLABEL

Γ ⊢ v : Labeled ℓ a

Γ ⊢ unlabel v : HLIO () ℓ1 (ℓ1 ⊔ ℓ) a

TO Labeled

Γ ⊢ m : HLIO ℓ1 ℓ2 a

Γ ⊢ toLabeled m : HLIO ℓ1 ℓ1 (Labeled ℓ a)

DEFER

Γ ⊢ m : HLIO ℓ1 ℓ2 a

Γ ⊢ defer m : HLIO ℓ1 ℓ1 a
```

---

for `labelOf`, but we elide the details since they are not relevant for our purposes. The semantics uses Felleisen-style evaluation contexts to specify evaluation order, where `Ep` stands for contexts for pure computations and `E` stands for contexts for effectful ones. As usual, we define →* to be the reflexive and transitive closure of →. Additionally, our transitions are labeled by the information-flow constraints that are being checked at runtime, as can be seen in rule (LABEL). We write `A →* B` if `A →* B` while performing the set of security checks `c`. For technical reasons, we also include a nonstandard primitive `eval` which is used to force pure computations. Despite not being a part of LIO, we remark that it acts on pure values and its evaluation involves no security-relevant effects, so it is easy to prove that the calculus is still sound after adding it. Essentially, LIO already includes a way to force evaluation for booleans (if statements), so `eval` is merely a generalization of this construct.

7.2 Semantics for HLIO

Figure 9 introduces the functions `interp` and `toLIO`, which we use to interpret HLIO and relate this interpretation with the corresponding standard LIO semantics. These two functions are defined as term-to-term transformations. The returned term, however, only utilizes LIO primitives. (Function `interp` closely follows the definition of function `go` described in Section 6.)

The function `interp` provides an interpretation of HLIO in dynamic LIO (Stefan et al. 2012b). Given a well-typed HLIO computation `m`, `interp m` runs `m` without performing any security checks, except for those in `deferrable`. This fact can be seen in the deferrable.
This case simply synthesizes a labeled term \((\text{Labeled}^{\text{TCB}} \ell t)\), thus skipping any security check. The \text{unlabel} operation performs no security checks, so its interpretation is exactly the same as in LIO.

The interpretation of labeled terms is cast into dynamic constraints and checks all of them at runtime, aborting the program if any of them fails. These constraints are checked in one go, before running the subcomputation itself. The static version of \text{toLabeled} is translated into its dynamic counterpart, where the final current label (after executing \(m\)) is predicted to be \(\ell_0\). The interpretation of \((\gg=)\) simply applies \text{interp} to its arguments.

Different from \text{interp}, the function \text{toLIO} directly translates an HLIO computation into a dynamic LIO computation where all the security checks occur dynamically. The translation for labeled terms, \text{toLabeled}, and \((\gg=)\) are defined similarly as in \text{interp}. Label and unlabel, however, simply reformulate the command in LIO, where the corresponding security side-effects might be triggered.

7.3 Non-interference

We define the simulation relation \(\sim\), which expresses that two terminating programs perform the same information flow checks and compute the same values.

**Definition 1.** (Simulation between LIO terms) Let \(A\) and \(B\) be LIO configurations, then \(A \sim B\) iff \(A \xrightarrow{*} X\) and \(B \xrightarrow{*} X\), where \(X\) is \(A\)'s weak head normal form. Note that we only consider terminating programs due to the fact that LIO only provides security guarantees for terminating runs.

We define a big-step evaluation relation \(\downarrow\) for HLIO terms.

**Definition 2.** (Big-step semantics for HLIO) Given an HLIO term, \((t : \text{HLIO} \ c \ell_1 \ell_0 \tau) \downarrow v\) if and only if \((\ell_1 \mid \text{interp} t) \xrightarrow{*} (\ell_0 \mid \text{toLIO} v)\).

The definition leverages the LIO semantics. It applies \text{interp} to the term being reduced as well as \text{toLIO} to the result. Observe that \text{toLIO} is needed for cases where \(v\) still contains HLIO terms, e.g., when \(v\) is composed of nested labeled terms.

The next lemma (see details in the extended version of the paper (Buijas et al. 2015)) introduces a relationship between the security checks done by HLIO and LIO.

**Lemma 1** (Simulation between HLIO and LIO terms). Given that \((t : \text{HLIO} \ c \ell_1 \ell_0 \tau) \downarrow v\), then \((\ell_1 \mid \text{guards} c \gg \text{interp} t) \sim (\ell_1 \mid \text{toLIO} t)\).

The lemma states that if we take the statically-determined constraints \(c\) for a well-typed term \(t\) into account, we can prove that the programs \(\text{guards} c \gg \text{interp} t\) and \(\text{toLIO} t\) are in simulation with respect to their security checks and final values. The former performs all statically-determined security checks in the beginning, and then runs the program with the deferred checks. The latter is obtained by viewing the original program as an LIO program, where all \text{defer} operations are removed.

The semantic correspondence from Lemma 1 guarantees that if an HLIO program is well-typed and terminates successfully, then the equivalent LIO program would also terminate successfully. Conversely, if the LIO program fails with a security error, the HLIO program will either not have a type or fail during a \text{defer} computation. Since the HLIO and LIO enforcement mechanisms are equivalent in this sense, and LIO enforces noninterference (Stefan et al. 2011b), we can show that HLIO enforces the same property.

For our security guarantees, we consider an attacker at sensitivity level \(t\), who can only observe values at a security level at most \(t\). LIO defines two terms \(\ell_2 \leq \ell_1\) and \(\ell_2 \leq \ell_1\) to be \(l\)-equivalent (written \((\ell_1 \approx \ell_2)\)) if the attacker is unable to distinguish between them, e.g., \(\text{Labeled}^{\text{TCB}} \ L 3 \approx \text{Labeled}^{\text{TCB}} \ L 5\) and \(\text{Labeled}^{\text{FCG}} \ H 1 \approx \text{Labeled}^{\text{TCB}} \ H 5\), but \(\text{Labeled}^{\text{FCG}} \ L 2 \not\approx \text{Labeled}^{\text{TCB}} L 1\). LIO also extends this notion to configurations. We leverage LIO definitions to express our non-interference theorem—after all, HLIO gets interpreted in LIO!

Noninterference expresses the notion that a program cannot leak secrets. Intuitively, a program is noninterfering if, considering two independent runs with \(l\)-equivalent inputs, their final values are also \(l\)-equivalent. In other words, attackers cannot distinguish the values of secret inputs by observing the outputs.
Theorem 1 (Termination-insensitive noninterference). Given HLIO terms $t_1$ and $t_2$ with no constructors, such that constraints $c_1$ and $c_2$ hold, $(t_1 : \text{HLIO} c_1 \ell_1 \ell_1 \tau_1 \triangleleft v_1; (t_2 : \text{HLIO} c_2 \ell_2 \ell_2 \tau_2) \triangleright v_2$, and $(\ell_1 \mid \text{toLIO} t_1) \approx_1 (\ell_1 \mid \text{toLIO} t_2)$, then it holds that $(\ell_1 \mid \text{toLIO} v_1) \approx_1 (\ell_2 \mid \text{toLIO} v_2)$.

Proof Sketch 1. The proof uses Lemma 1 to relate the reductions of $\text{interp} t_1$ and $\text{ interp} t_2$ with $\text{toLIO} t_1$ and $\text{toLIO} t_2$, respectively. Once that is done, the result follows by applying the LIO non-interference theorem in (Stefan et al. 2012b). This theorem requires that $t_1$ and $t_2$ do not include constructors of the form $\text{LJoin}$. Consequently, observe that it is not possible to directly consider l-equivalence between interpreted terms, i.e., $\text{interp} t_1$ and $\text{interp} t_2$—they introduce constructors $\text{LJoin}$ to avoid security checks. The proof is given in the extended version of the paper (Buiras et al. 2015).

Theorem 1 indicates that $l$-equivalent (fully) dynamic interpretations of HLIO terms (i.e., $(\ell_1 \mid \text{toLIO} t_1) \approx_1 (\ell_1 \mid \text{toLIO} t_2)$), where the static checks hold, produce l-equivalent results (in LIO) (i.e., $(\ell_2 \mid \text{toLIO} v_1) \approx_2 (\ell_2 \mid \text{toLIO} v_2)$). Observe that if any HLIO terms leaked secrets, $l$-equivalence involving $v_1$ and $v_2$ would not hold.

8. Discussion
This section explains some design choices, while exploring others.

The toLabeled Function The HLIO type for toLabeled deserves some attention. From Section 2, we know that toLabeled $\ell$ in LIO performs two security checks: $\ell_{\text{eq}} \equiv \ell$ at the beginning of toLabeled, and $\ell_{\text{eq}} \equiv \ell$ where $\ell_{\text{eq}}$ is the current label obtained by evaluating $\alpha$. A directly corresponding static version of toLabeled (and its dynamic checks) might be:

toLabeled :: Label $\ell \rightarrow$ HLIO $c \ell_1 \ell_0 a$

\rightarrow HLIO $(c, \text{FlowsE} \ell_1 \ell, \text{FlowsE} \ell_0 \ell) \ell_1 \ell_1$ (Labeled $\ell a$)

Recall that, for security reasons, the role of the first argument of type Label $\ell$ is to statically predict an upper bound of the current label obtained by running $m$. The constraints in the return type of toLabeled express this fact. In HLIO, however, that prediction is already given! Observe that type $m :: \text{HLIO} c \ell b a$ says “after running $m$, the final current label is $\ell_b$.” We can use $\ell_b$ as the upper bound, i.e., $\ell \equiv \ell_b$, and remove the static check FlowsE $\ell_0 \ell$. Moreover, we know that $\ell_0 \subseteq \ell_b$ by construction, which allows the removal of FlowsE $\ell_0 \ell$. By taking all these facts together, we can dismiss all the extra constraints.

toLabeled :: HLIO $c \ell_1 \ell_0 a \rightarrow$ HLIO $c \ell_1 \ell_1$ (Labeled $\ell_1 a$)

In Section 7, we have formally proved that this primitive is secure by establishing a simple relationship with its counterpart in LIO.

Conditionals The monad HLIO is embedded in Haskell as a GADT, so it is possible to use Haskell’s if statements to express conditional branching. However, the Haskell type system requires that the types of both branches be the same. In particular, if the branches are HLIO computations, their types must also completely agree, including constraints and initial and final labels. Unfortunately, this means that it is not possible to have if statements where one branch produces a constraint and the other one does not; more generally, where the branches produce different sets of constraints. For example, the following expression, where $x :: \text{Int}$, is ill-typed:

if $x > 0$ then (label $H x \gg return x$) else return $(x + 1)$

The reason for the type error is that one branch has type HLIO $(\text{Flows} \ell_1 H) \ell_1 \ell_1 \text{Int}$, while the other one has type HLIO $(\text{Flows} \ell_2 H) \ell_2 \ell_2 \text{Int}$. When it comes to disparities in the constraints, it is possible to work around this restriction by means of defer operations. The programmer can use defer to check one or both of the branches dynamically, which causes the constraints in the HLIO type to be $(\cdot)$, thus keeping the Haskell type checker happy. However, if the current label is not updated in exactly the same way in both branches, the if statement will also be ill-typed. Note that this cannot be solved with defer.

An alternative solution that addresses the problem with both constraints and the current label involves adding another primitive for if statements, i.e., a constructor If for the HLIO GADT. The type of this constructor would accurately express the connection between constraints and current labels in both branches, as follows:

If :: Bool $\rightarrow$ HLIO $c_1 \ell_1 \ell_0 a \rightarrow$ HLIO $c_2 \ell_2 \ell_0 a$

\rightarrow HLIO $(c_1, c_2) \ell_i (\text{LJoin} \ell_0 \ell_0 a)$

Essentially, the primitive would over-approximate the constraints and the final label, as can be expected from a static analysis. This solution would not only introduce notational overhead but also complicate the formal treatment of HLIO significantly, as we would no longer have a one-to-one correspondence between static and dynamic checks. Instead, we could prove that the dynamic checks are a subset of the statically-determined constraints. In order to simplify our exposition, we chose to avoid this solution, but we believe it would be a reasonably straightforward extension.

Deferring Constraints beyond Non-interference The Deferrable type class enables programmers to give instances for deferring the check for a constraint to runtime. In this section, we show how to push this idea to the extreme, by deferring the check for type equalities that are generated by GHC’s type inference. We iterate that the code in this section (and everywhere in this paper) requires no modifications to GHC.

We wish to defer a type equality between two types $ta$ and $tb$, which in GHC type system would be expressed as $ta \sim tb$ of kind Constraint. Of course, in order to perform such a test at runtime, we need to have runtime type information around about the shape of types $ta$ and $tb$. GHC provides the Typeable type class that captures runtime type representations. This enables the following instance definition:

instance (Typeable $a$, Typeable $b$) $\Rightarrow$
Deferrable $(a \sim b)$ where defer $p \; m = \text{case } eqT \; x$ of Nothing $\rightarrow$ error ""type error!"
Just Refl $\rightarrow m$

Function eqT is a standard library function, providing a runtime witness of the equality of two types that are instances of Typeable:

eqT :: (Typeable $b$, Typeable $a$) $\Rightarrow$ Maybe (a $\sim b$)

and $a \sim b$ is a GADT expressing with its only constructor Refl the fact that $a$ and $b$ are in fact equal:

data (a $\sim b$) where Refl :: (a $\sim b$) $\Rightarrow$ (a $\sim b$)

If programmers write a program that contains a type error:

foo :: forall $a$ $a$ $\rightarrow$ $a$ $\rightarrow$ $a$
foo $x$ $y$ $\leftarrow$ if $x$ then False else $y$

GHC will report: Couldn’t match expected type ‘Bool’ with actual type ‘a’. As we may, in fact, apply foo to two boolean values at runtime, programmers may want to make this program typeable by deferring the constraint:

foo :: forall $a$. Typeable $a$ $\Rightarrow$ a $\rightarrow$ a $\rightarrow$ a
foo $x$ $y$ $\leftarrow$ defer $p$ (if $x$ then False else $y$)

where $p ::$ Proxy (a $\sim$ Bool) $\perp$
In this case, \texttt{foo True False} returns \texttt{False}, while \texttt{foo 3 4} produces a \texttt{Exception: type error}. Note that this behavior differs from related work (Vytiniotis et al. 2012), which defers unsatisfiable constraints as errors to runtime. Instead, we do genuinely defer the check at the (unavoidable) cost of having the type representation around.

9. Related work

Hybrid IFC There is considerable literature on static analyses aiding IFC execution monitors for different purposes. To boost permissiveness, Le Guernic et al. provide monitors which statically analyze non-taken branches of secret conditionals (Le Guernic et al. 2007; Le Guernic 2007). Similarly, Shroff et al. design a monitor which leverages variable dependencies (provided by a type system) when programs branch on secrets (Shroff et al. 2007). Besides permissiveness, hybrid analyses are used to avoid leaks in dynamic flow-sensitive IFC monitors, where variables change their security levels at runtime based on what data they store (Russo and Sabelfeld 2010). Moore and Chong utilizes static analysis to avoid tracking variables which do not impose security violations, thus improving performance on dynamic monitors (Moore and Chong 2011). Jif, an IFC-aware compiler for Java programs, supports dynamic labels to classify data based on runtime observations (Zheng and Myers 2007). Similar to our work, operations on labels are modeled at the level of types. In the dynamic part, however, they only allow for runtime checks based on the \(\sqsubseteq\) relationship. As in this work, there is some literature which connects dynamic and static analysis at the programming-language level. Disney and Flanagan describe an IFC type-system for a pure calculus which defers cast checks to runtime when they cannot be determined statically (Disney and Flanagan 2011). Luminous and Thiennann extend that work to consider references (Fennell and Thiennann 2013).

Security Libraries Li and Zdancewic’s seminal work (Li and Zdancewic 2006) shows how arrows (Hughes 2000) can provide IFC without runtime checks as a library in Haskell. Tsai et al. (Tsai et al. 2007) extend Li and Zdancewic’s work to support concurrency and data with multiple security labels. Rather than using arrows, Russo et al. (Russo et al. 2008) shows that monads are capable of providing a library which statically enforces IFC. Devriese and Piessens provide a monad transformer to extend imperative-like APIs with support for IFC. Their technique is applied to dynamic, static, and hybrid IFC techniques. Devriese and Piessens’ work requires a deep embedding of the target language in order to perform static analysis. In contrast, our approach leverages the type-system features found in Haskell. Jaskelioff and Russo implement a library which dynamically enforces IFC using secure multi-execution (SME) (Jaskelioff and Russo 2011)—a technique that runs programs multiple times (once per security level) and varies the semantics of inputs and outputs to protect confidentiality. The series of work on LIO can be referred to as the state-of-the-art in dynamic IFC in Haskell (Stefan et al. 2011b, 2012a; Buiras et al. 2013; Buiras and Russo 2013; Buiras et al. 2014).

Programming Languages Combining dynamic and static analysis is not exclusive to IFC research. It has been extensively studied by the programming languages community. We briefly mention some highlights and their relation to this work. Flanagan (Flanagan 2006) develops the concept of \textit{hybrid type checking} for type systems capable of delaying subtyping checks until runtime. Siek and Taha (Siek and Taha 2006) coined the term \textit{gradual typing}, which applies when programmers can control the combination of static and dynamic approaches at the programming language level—simultaneously, Hochstadt and Felleisen (Hochstadt and Felleisen 2006) introduce similar ideas. Due to the \textit{def er} primitive, HLIO can be considered as a simple gradual typing system. Wadler and Findler (Wadler and Findler 2009) presents the idea of \textit{blame} to explain failure of dynamic type casts (specially for languages with higher-order functions). HLIO is a system which only produces positive blame. Recently, the idea of gradual typing has gained popularity among several programming languages. Typed Scheme (Hochstadt and Felleisen 2006) and Racket (Takikawa et al. 2012) allow Scheme programmers to decorate their code with type annotations. Reticulated Python (Vitousek et al. 2014) implements gradual typing, where a type checker is provided in combination with a code-to-code transformation into Python 3. JavaScript has been also a recent target of this kind of systems (Swamy et al. 2014; Rastogi et al. 2015). Different from these approaches, HLIO does not provide a fully-fledged gradual typing system. On the other hand, it avoids any compiler modification by leveraging Haskell’s powerful type system.

10. Conclusions and Future Work

We have presented HLIO, a new hybrid IFC enforcement in Haskell that allows programmers to defer static constraints to runtime. This feature is particularly useful, for instance, in production systems—where it is often the case that security labels are not available (or even known) at compile time. Different from other programming languages, GHC’s powerful type-system and features allowed us to build HLIO as a simple library, where no runtime or compiler modifications were needed. On formal aspects, we showed that the library satisfies termination-insensitive non-interference for an arbitrary security lattice.

As part of developing HLIO, we have identified an independently useful technique for deferring other forms of static constraints, including ordinary type equalities. In future work, we aim to explore the use of these techniques in languages with similarly expressive type systems, such as dependently typed languages. In addition, we plan to further explore the design and application space of these techniques, and explore their usability in embedded domain-specific languages and code generators.

Acknowledgments

This work was funded by DARPA CRASH under contract #N66001-10-2-4088, and the Swedish research agencies VR and the Barbro Osher Pro Suecia foundation. We thank the anonymous reviewers and Bart van Delft for useful comments and suggestions.

References


P. Buiras, D. Vytiniotis, and A. Russo. HLIO: Mixing Static and Dynamic Typing for Information-Flow Control in Haskell.
