DoCoMo USA Labs Technical Report DCL-TR-2005-0002

A Typed Assembly Language for Confidentiality

Dachuan Yu Nayeem Islam
DoCoMo Communications Laboratories USA
{yu,nayeem}@docomolabs-usa.com

Abstract

Language-based information-flow analysis is promising in protecting data confidentiality. Although much work has been carried out in this area, relatively little has been done for assembly code. Techniques at a source level do not generalize straightforwardly to assembly code, because assembly code does not readily present certain abstraction about the program structure that is crucial to information-flow analysis. Nonetheless, low-level information-flow analysis is desirable, because it yields a small trusted computing base. Furthermore, many (untrusted) applications are distributed in native code; their verification should not be overlooked.

We present a simple yet effective solution for this problem. Our observation is that the missing abstraction in assembly code can be restored using annotations. Following the philosophy of certifying compilation, these annotations are generated by a compiler, used for static validation, and erased before execution. In particular, we propose a type system for low-level information-flow analysis. Our system is compatible with Typed Assembly Language, and models key features including a call stack, memory tuples and first-class code pointers. A noninterference theorem articulates that well-typed programs respect confidentiality. We also present a security-type preserving translation that targets our system, together with its soundness theorem. This illustrates the application of certifying compilation for noninterference.

1. Introduction

With the growing reliance on networked information systems, the protection of confidential data becomes increasingly important. The problem is especially subtle for a computing system which both manipulates sensitive data and requires access to public information channels. Simple policies that restrict the access to either the sensitive data or the public channels (or a combination therefrom) often prove too restrictive. A more desirable policy is that no information about the sensitive data can be inferred from observing the public channels, even though a computing system is granted access to both. Such a regulation of the flow of information is often referred to as *information flow*, and the policy that sensitive data should not affect public data is often called *noninterference*.

Whereas it is relatively easy to detect and prevent naive violations that directly give out sensitive data, it is much more difficult to prevent applications from sending out information that is sophisticatedly encoded. Conventional security mechanisms such as access control, firewalls, encryption and anti-virus fall short on enforcing the noninterference policy [23]. On the one hand, noninterference posts seemingly conflicting requirements: it allows the access to sensitive information, but restricts the flow of it. On the other hand, the violation of noninterference cannot be observed from monitoring a single execution of the program [25], yet such execution monitoring is the basis of many conventional mechanisms.

In recent years, much effort has been put on enforcing noninterference using techniques based on programming language theory and implementation. These techniques are promising, because they directly inspect or instrument the program code, and hence have the potential of learning all possible run-time behavior of the program. Unfortunately, the vast amount of language-based research on information flow [23] does not address well the problem for assembly code. The challenge there, as we will elaborate later, largely lies in working with the lack of high-level abstractions and managing the extreme flexibility offered by assembly code.

Nonetheless, it is desirable to enforce noninterference directly at a low-level. On the one hand, high-level programs must be translated into low-level code before executed on a real machine; compilation or optimization bugs may invalidate the security guarantee established for the source programs. On the other hand, some applications are distributed (*e.g.*, native code for mobile computation) or even directly written (*e.g.*, core libraries for embedded systems) in assembly code; enforcement at a low-level is a must for them.

This paper presents some important steps of a project tackling information flow at the assembly level. The contributions are:

- We propose a Typed Assembly Language for Confidentiality (TAL_C) for information-flow analysis and present its proof of noninterference. Our abstract machine is generic and close to real architectures. To reuse existing results on low-level verification, our system is designed to be compatible with Typed Assembly Language (TAL) [18]. It thus approaches a unified framework for conventional type safety and security.
- Our system models key features of an assembly language, including heap, call stack and register file, memory tuples (aliasing), and first-class code pointers (higher-order functions). Because assembly code is often arduous to work with, we present our formal result with a core language supporting the above features for ease of understanding, but also informally discuss extensions such as polymorphic and existential types.
- Although desirable to directly verify at an assembly level, it is more practical to develop programs in high-level languages. We present a translation from a security-typed imperative source language with first-order procedures to TAL_C. This illustrates the application of certifying compilation for noninterference. We also present a type-preservation theorem for our translation.

This paper does not address covert channels (*e.g.*, termination [28, 1] and timing [30, 2]) or abstract-violation attacks (*e.g.*, cache [3]). Section 2 provides background on language-based approaches for information flow, places our work in the context of existing researches, and points out the extra difficulties for noninterference at an assembly level. An informal overview of our approach is given in Section 3. Sections 4 and 5 present the TAL_C system and a certifying compilation scheme, focusing on core features that illustrate ideas pertinent to information flow. Section 6 helps better understand TAL_C in comparison with previous work on linear continuations. Orthogonal issues and practical extensions are discussed in Section 7. Section 8 concludes.

2. Background

2.1 Information Flow

The problem of information flow can be abstracted as a program that operates on data of different security levels, *e.g.*, *low* and *high*. Low (low security) data are public data that may be observed by all principals; high (high security) data are secret data whose access is restricted. An information-flow policy requires that no information about high inputs can be inferred from observing low outputs. In general, the security levels can be generalized to a lattice [29].

Such a policy concerns tracking the flow of information inside a target system. Whereas it is easy to detect explicit flows (*e.g.*, through an assignment from a secret `h` to a public `l` with `l=h`), it is much harder to detect various forms of implicit flow. For example, the statement `l=0; if h then l=1` involves an implicit flow from `h` to `l`. At run-time, if the `then` branch is not taken, a conventional security mechanism based on execution monitoring will not detect any violation. However, information about `h` can indeed be inferred from the result of `l`.

Instead of observing a single execution, language-based techniques derive assurance about a program's behavior by examining, and possibly instrumenting, the program code. In the above example, the information essentially leaks through the program counter (often referred to as *pc*)—the fact that a branch is taken reflects information about the guard of the conditional. In response, a security-type system typically tags the program counter with a security label. If the guard of a conditional concerns high data, then the branches are verified under a program counter with a high security label. Furthermore, assignments to low variables are prohibited under such a high program counter.

2.2 Security Types

Figure 1 shows a two-level security-type system for a simple imperative language with first-order procedures. It is extended from a demonstrative system of Sabelfeld and Myers' [23], and will serve as the source of our translation. A program comprises a list of procedure declarations $\mathtt{F}_i$ and a main command `C`. A procedure declaration documents the security level of the program counter with `pc`, indicating that the procedure body will only update variables with security levels no less than `pc`. A procedure also declares a list of arguments $\mathtt{x}_i$ under call-by-reference semantics. Commands `C` consist of assignments, sequential compositions, conditional statements, while-loops, and procedure calls. Variables `V` cover both global variables `v` and procedure arguments `x`. Expressions `E` are formed by constants (`i`), variables, and their additions.

Rules [E1–4] relate expressions to security types (levels). Any expression may have type `high` (it is secure to treat any data as sensitive). Constants and low variables may have type `low`. An addition expression may have type `low` if both sub-expressions may have type `low`.

Rules [C1–7] track the security level of the program counter (`pc`) when verifying the commands. Assignments to high variables are always valid (Rule [C1]). However, an assignment to a low variable is valid only if both the expression and the `pc` are low (Rule [C2]). For a conditional (Rule [C3]), the security level of the sub-commands must match the security level of the guard expression; together with Rule [C2], this guarantees that low variables are not modified within a branch under a high guard. After a conditional, it is useful to reset the `pc` to low, avoiding a form of label creep [10] where monotonically increasing security labels are too restrictive to be generally useful. Such a context reset is achieved with a subsumption rule (Rule [C4]); intuitively, if it is secure to execute a command in a sensitive context, then it is also secure in an insensitive one. A sequential composition is verified so that both sub-commands are valid under the given `pc` (Rule [C5]). The handling of a while-loop is similar to that of a conditional statement (Rule [C6]). A procedure call is valid if `pc` matches the expected security level, and the arguments have the expected types (Rule [C7]); note that only variables (`v` or `x`) may server as the arguments, which are handled by reference (also know as "in-out" arguments in the previous work of Volpano and Smith [29]).

Finally, a procedure declaration is valid if the body can be verified under the expected `pc` and arguments (Rule [F1]). A program is valid if all procedure declarations and the main command are valid (Rule [P1]).

(*Typ*) $\mathtt{t},\mathtt{pc} ::= \mathtt{low} \mid \mathtt{high}$

(*Var*) $\mathtt{V} ::= \mathtt{v} \mid \mathtt{x}$

(*Env*) $\Phi ::= \circ \mid \mathtt{V}:\mathtt{t},\Phi \mid \mathtt{f}:\langle\mathtt{pc}\rangle(\mathtt{t}_1,\ldots,\mathtt{t}_n)\to\mathtt{void},\Phi$

(*Exp*) $\mathtt{E} ::= \mathtt{i} \mid \mathtt{V} \mid \mathtt{E}_1 + \mathtt{E}_2$

(*Comm*) $\mathtt{C} ::= \mathtt{V} := \mathtt{E} \mid \mathtt{C}_1;\mathtt{C}_2 \mid \mathtt{if}\ \mathtt{E}\ \mathtt{then}\ \mathtt{C}_1\ \mathtt{else}\ \mathtt{C}_2 \mid \mathtt{while}\ \mathtt{E}\ \mathtt{do}\ \mathtt{C} \mid \mathtt{f}(\mathtt{V}_1,\ldots,\mathtt{V}_n)$

(*Fun*) $\mathtt{F} ::= \mathtt{f}\langle\mathtt{pc}\rangle(\mathtt{x}_1:\mathtt{t}_1,\ldots,\mathtt{x}_n:\mathtt{t}_n)\{\mathtt{C}\}$

(*Prog*) $\mathtt{P} ::= \{\mathtt{F}_1;\ldots;\mathtt{F}_n;\mathtt{C}\}$

[E1–2] $\Phi \vdash \mathtt{E} : \mathtt{high}$ $\qquad$ $\Phi \vdash \mathtt{i} : \mathtt{t}$

[E3–4] $\dfrac{\Phi(\mathtt{V}) = \mathtt{low}}{\Phi \vdash \mathtt{V} : \mathtt{low}}$ $\qquad$ $\dfrac{\vdash \mathtt{E}_1 : \mathtt{low} \quad \vdash \mathtt{E}_2 : \mathtt{low}}{\vdash \mathtt{E}_1 + \mathtt{E}_2 : \mathtt{low}}$

[C1–2] $\dfrac{\Phi(\mathtt{V}) = \mathtt{high}}{\Phi;[\mathtt{pc}] \vdash \mathtt{V} := \mathtt{E}}$ $\qquad$ $\dfrac{\Phi(\mathtt{V}) = \mathtt{low} \quad \Phi \vdash \mathtt{E} : \mathtt{low}}{\Phi;[\mathtt{low}] \vdash \mathtt{V} := \mathtt{E}}$

[C3] $\dfrac{\Phi \vdash \mathtt{E} : \mathtt{pc} \quad \Phi;[\mathtt{pc}] \vdash \mathtt{C}_1 \quad \Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{if}\ \mathtt{E}\ \mathtt{then}\ \mathtt{C}_1\ \mathtt{else}\ \mathtt{C}_2}$

[C4–5] $\dfrac{\Phi;[\mathtt{high}] \vdash \mathtt{C}}{\Phi;[\mathtt{low}] \vdash \mathtt{C}}$ $\qquad$ $\dfrac{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1 \quad \Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1;\mathtt{C}_2}$

[C6] $\dfrac{\Phi \vdash \mathtt{E} : \mathtt{pc} \quad \Phi;[\mathtt{pc}] \vdash \mathtt{C}}{\Phi;[\mathtt{pc}] \vdash \mathtt{while}\ \mathtt{E}\ \mathtt{do}\ \mathtt{C}}$

[C7] $\dfrac{\Phi(\mathtt{f}) = \langle\mathtt{pc}\rangle(\mathtt{t}_1,\ldots,\mathtt{t}_n)\to\mathtt{void} \quad \Phi \vdash \mathtt{V}_i : \mathtt{t}_i \quad \forall i \in \{1\ldots n\}}{\Phi;[\mathtt{pc}] \vdash \mathtt{f}(\mathtt{V}_1,\ldots,\mathtt{V}_n)}$

[F1] $\dfrac{\mathtt{x}_1:\mathtt{t}_1,\ldots,\mathtt{x}_n:\mathtt{t}_n,\Phi;[\mathtt{pc}] \vdash \mathtt{C}}{\Phi \vdash \mathtt{f}\langle\mathtt{pc}\rangle(\mathtt{x}_1:\mathtt{t}_1,\ldots,\mathtt{x}_n:\mathtt{t}_n)\{\mathtt{C}\}}$

[P1] $\dfrac{\mathtt{F}_i = \mathtt{f}_i\langle\mathtt{pc}_i\rangle(\mathtt{x}_{1i}:\mathtt{t}_{1i},\ldots,\mathtt{x}_{n_i i}:\mathtt{t}_{n_i i})\{\mathtt{C}_i\} \quad \Phi(\mathtt{F}_i) = \langle\mathtt{pc}\rangle(\mathtt{t}_{1i},\ldots,\mathtt{t}_{n_i i})\to\mathtt{void} \quad \Phi \vdash \mathtt{F}_i \quad \Phi;[\mathtt{low}] \vdash \mathtt{C} \quad \forall i \in \{1\ldots n\}}{\Phi \vdash \{\mathtt{F}_1;\ldots;\mathtt{F}_n;\mathtt{C}\}}$

Figure 1. A simple security-type system

2.3 Related Work

Although there has been much work applying language-based techniques to information flow [23], most of it focused on high-level languages. Many high-level abstractions have been formally studied, including functions [11], exceptions [22], objects [6], and concurrency [27, 1, 12], and practical implementation is within reach [19]. Nonetheless, enforcing information flow at only a high level puts the compiler into the trusted computing base (TCB) [24]. Furthermore, we should not overlook the verification of software distributed (or written) directly in low-level code. For example, a user may wish to verify that a GPS software, downloaded from an untrusted party in the form of native code to a mobile device, does not send out the location information through the network.

Barthe *et al.* [7] presented a security-type system for a bytecode language and a translation that preserves security types. Their stack-based language is much different from the RISC architecture that we model. More importantly, their verification circumvents a main difficulty—the lack of program structures at a low-level—by introducing a (currently trusted) component that computes the dependence regions and postdominators [5] for conditionals. The separate checking of these information is under investigation.

Avvenuti *et al.* [4] applied abstract interpretation to enforce information flow for a stack-based bytecode language. Besides the difference in the machine models, their work also relied on the (trusted) computation of control flow graphs and postdominators.

Zdancewic and Myers [33] used linear continuations to enforce noninterference at a low-level. Their language is based on variables and still much different from assembly language. In particular, linear continuations, although useful in enforcing a stack discipline that helps information-flow analysis, are absent from conventional assembly code. Hence further (trusted) compilation to native code is required. Nonetheless, we borrowed some ideas from Zdancewic and Myers, including the handling of memory aliasing and code pointers, although these features are modeled as different constructs in our system. A more thorough discussion of the connection between linear continuations and our solution is given in Section 6, after presenting our system.

Bonelli *et al.* [8] explored the realization of linear continuations in an assembly language SIFTAL. Two new instructions are introduced in correspondence with the operations on linear continuations as proposed by Zdancewic and Myers [33]. These two instructions enforce structured control flows that are missing from normal assembly code with the help of a continuation stack (this stack is different from the one for function calls). One instruction pushes a linear continuation onto the stack, the other pops a linear continuation off the stack and transfers the control to it. Such a mechanism maintains structured control flow in assembly code, thus helps information-flow analysis. Unfortunately, conventional assembly programming and machine models do not contain such a special continuation stack and the instructions manipulating it.

Recently, Medel *et al.* [16] improved SIFTAL to SIF, using a stack of labels to simplify the above approximation of linear continuations. Unlike SIFTAL, SIF resorts to static type annotations to enforce noninterference, and no longer requires a stack of linear continuations during execution. This is in spirit similar to our solution of TAL_C. However, SIF supports only a minimal set of language features (arithmetic, memory update, branching and direct jumps), and does not address how the type annotations can be produced. In contrast, our language TAL_C further supports code pointers and a call stack. We also present a type-preserving translation to TAL_C from a security-typed source language, where the support for procedure calls introduces extra subtleties for noninterference. We will discuss this in more detail in Section 6.

This paper targets RISC-style assembly code. We introduce a type system to verify the unstructured control flow, which in turn helps information-flow analysis. Type annotations are used to recover information about high-level program structures, and no trusted component is required for computing postdominators. This contrasts with the above work on bytecode languages. Furthermore, we do not rely on extra constructs such as linear continuations or a continuation stack. An erasure semantics trivially reduces programs in our language to normal assembly code.

We also provide a formal model of a certifying compiler for noninterference. Certifying compilation [14] has mostly been studied for conventional type safety (*e.g.,* Typed Assembly Language [18], Proof-Carrying Code [21, 20] and Efficient Code Certification [13]). Walker [31] applied certifying compilation to security policies. However, being based on security automata, Walker's system cannot enforce noninterference. Besides the work on security-type preserving compilation by Barthe *et al.* [7] as discussed above, Honda and Yoshida [12] also studied related issues for π-calculus with security types.

2.4 Assembly Code

Whereas enforcing information flow for assembly code is important, it poses many new challenges.

First, high-level languages make use of a virtually infinite number of variables, each of which can be assigned a fixed security label. In assembly code, the use of memory cells is similar. However, a finite number of registers are reused for different source-level variables. As a result, one cannot assign a fixed security label to a register.

Second, the control flow of an assembly program is not as structured. The body of a conditional is often not obvious, and generally undecidable, from the program code. Hence the idea of using a security context to prevent implicit flow through conditionals cannot be easily carried out.

Third, assembly languages are very expressive. Aliasing between memory cells are difficult to reason about [26]. The support for first-class code pointers (the reflection of higher-order functions at the assembly level) is very subtle. A code pointer may direct a program to different execution paths, even though no branching instruction is present.

Fourth, since it is not practical to always directly program in an assembly language, a low-level type system must be designed so that the type annotations can be generated automatically, *e.g.,* through certifying compilation. The type system must be at least as expressive as a high-level type system, so that any well-typed source program can be translated into well-typed assembly code.

Finally, it is desirable to achieve an erasure semantics where type annotations have no effect at runtime. A security mechanism can not be generally applied in practice if it incurs too much overhead. Similarly, it is also undesirable to change the programming model for accommodating the verification needs. Such a model change indicates either a trusted compilation process or a different target machine.

3. Our Approach

3.1 Explicit Assignment

An obvious kind of information flow is through assignment. As discussed in Section 2.2, variables in a high-level language can be "tagged" with security labels; the security-type system prevents label mismatch for assignments. At an assembly level, memory cells can be tagged similarly. When storing into a memory cell, a typing rule ensures that the security label of the source matches that of the target.

Registers need to be regulated differently, because they can be reused for different variables with different security labels (registers cannot be aliased, which makes it safe to update their types). Since variable and liveness information is not available at an assembly level, one can not easily base the enforcement upon that.

In fact, a similar problem arises even for normal type safety. A register in TAL can have different types at different program points. These types are essentially inferred from the computation itself. For instance, in an addition instruction $\texttt{add}\, r_d, r_s, r_t$, the register r_d is given the type `int`, because only `int` can be valid here. Similarly, when loading from a memory cell, the target register is given the type of the source memory cell. Adapting such inference for security labels is straightforward. In the addition $\texttt{add}\, r_d, r_s, r_t$, the label of r_d is obtained by joining the labels of r_s and r_t, because the result in r_d reflects information from both r_s and r_t. Moving and memory reading instructions are handled similarly.

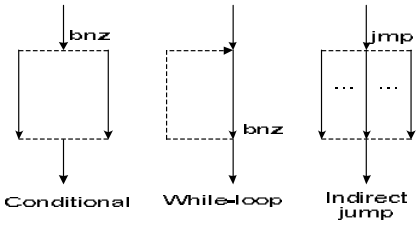

Figure 2. Flow through program structure

3.2 Program Structure

A conditional statement in a high-level program can be verified so that both sub-commands respect the security level of the guard expression. Such verification becomes difficult in assembly code, where the "flattened" control flow provides little help in identifying the program structure. A conditional is typically translated into a branching instruction (`bnz` r, l) and some code blocks, where the postdominator of the two branches are no longer apparent.

We use annotations to restore the program structure by pointing out the postdominators whenever they are needed. Note that high-level programs provide sufficient information for deciding the postdominators, and these postdominators can always be statically determined. For instance, the end of a conditional command is the postdominator of the two branches. Hence a compiler can generate the annotations automatically based on a securely typed source program. In our system, our postdominator annotation is essentially a static code label paired with a security label.

Since branching instructions (`bnz` r, l) are the only instructions that could directly result in different execution paths, it would appear that one should enhance branching instructions with postdominators. The typing rule then checks both branches under a proper security context that takes into account the guard expression. Such a security context terminates when the postdominator is reached.

Although plausible, this approach is awkward. Figure 2 demonstrates three scenarios. Besides the conditional scenario, branching instructions are also used to implement while-loops, where the postdominator is exactly the beginning of one of the branches. In this case, only the other branch should be checked under a new security context. If we directly annotate the branching instruction, the corresponding typing rule would be "overloaded." More importantly, an assembly program may contain "implicit branches" where no branching instruction is present. The third scenario illustrates that an indirect jump may lead the program to different paths based on the value of its operand register. A concrete example will appear in Section 3.5.

Inspiration of a better solution lies in the simple system of Figure 1. Note that the subsumption rule [C4] is not tied to any particular commands. It essentially marks a region of computation where the security level is raised from low to high. The end of the region is exactly a postdominator. Following this, our approach is to mimic the high-level subsumption rule with two low-level *raising* and *lowering* operations that explicitly manipulate the security context and mark the beginning and the end of the secured region.

3.3 Memory Aliasing

Aliasing of memory cells present another channel for information transfer. In Figure 3, a low pointer `p_l` and a high pointer `p_h` are aliases of the same cell. This is useful if a high principal wishes to observe a low computation. The code in this figure may change the aliasing relation based on some high variable `h` by letting `p_h` point to another cell. Further modification through `p_h` may or may not change the value in the original cell. As a result, observing through the low pointer `p_l` reveals information about the high variable `h`.

```
(* suppose p_h alias p_l *)
if (h=0) then p_h=new cell;
*p_h=1;
(* now *p_l reveals h *)
```

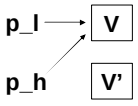

Figure 3. Flow through aliasing

```
fun f0 () = (l:=0; ())
fun f1 () = (l:=1; ())
let f = (if h then f1 else f0) in f()
```

Figure 4. Flow through code pointer

```
fun f0 () = (h':=0; ())
fun f1 () = (h':=1; ()) ...
if h then f := f1 else f := f0;
l:=1; !f(); l:=l*2; ...
```

Figure 5. Context coercion without branching

The problem lies in the assignment through the high pointer `p_h`, because it reveals information about the aliasing relation. The solution, following previous work [6, 33], is to tag pointers with two security labels. One is for the pointer itself, and the other is for the data being referenced. Assignments to low data through high pointers are not allowed. This is a conservative approach—all pointers are considered as potential aliases.

3.4 Code Pointers

Code pointers further complicate information flow. Figure 4 shows a piece of functional code where `f` represents different functions based on a high variable `h`. In its reflection at an assembly level, different code blocks will be executed based on the value of `h`. Naturally, `f` contains sensitive information and should be labeled high. However, the actual functions `f0` and `f1` can only be executed under a low context, because they modify a low variable `l`. In this case, the invocation to `f` should be prohibited.

In our system, similar to data pointers, code pointers are also given two security labels. The typing rules ensure that no low function is called through a high code pointer.

3.5 Security Context Coercion

Finally, Figure 5 shows a piece of code where a mutable code pointer complicates the flow analysis. Functions `f0` and `f1` only modify high data. A reference cell `f` is assigned different code pointers within a high conditional. Later, `f` is dereferenced and invoked in a low context.

This code is safe with respect to information flow. At a high level, a subsumption rule like Rule [C4] in Figure 1 allows calling the high function `!f()` in a low context. However, in its assembly counterparts, both the calling to `f` and the returning from `f` are implemented as indirect jumps. The calling sequence transfers the control from a low context to a high context, whereas the returning sequence does the opposite. Since the function invocation is no longer atomic at an assembly level, one cannot directly devise a subsumption rule. Furthermore, there is no explicit branching instruction present when `f` is dereferenced and invoked (the third scenario of Figure 2).

In our system, the raising and lowering operations explicitly mark the boundary of the subsumption rule. During certifying compilation, the source-level typing and program structure provide sufficient information for generating the target-level annotations. When a subsumption rule is applied in the source code, the corresponding target code is generated within a pair of raising and lowering operations.

$$
\begin{array}{rll}
\textit{(contexts)} & \kappa & ::= \bullet \mid \theta \triangleright w \\
\textit{(pre-type)} & \tau & ::= \mathtt{int} \mid \langle \sigma_1, \ldots, \sigma_n \rangle \mid \forall[\Delta].\langle \kappa \rangle\, \Gamma \\
\textit{(types)} & \sigma & ::= \tau_\theta \mid ns \\
\textit{(stack ty)} & \Sigma & ::= \rho \mid nil \mid \sigma :: \Sigma \\
\textit{(var env)} & \Delta & ::= \circ \mid \rho\Delta \mid \alpha\Delta \\
\textit{(type arg)} & \psi & ::= \Sigma \mid w \\
\textit{(heap ty)} & \Psi & ::= \{l_1 : \sigma_1, \ldots l_n : \sigma_n\} \\
\textit{(reg file ty)} & \Gamma & ::= \{r_1 : \sigma_1, \ldots r_n : \sigma_n, \mathtt{sp} : \Sigma\} \\
\\
\textit{(registers)} & r & ::= r_1 \mid r_2 \mid \ldots \\
\textit{(word val)} & w & ::= \alpha \mid l \mid i \mid ns \mid w[\psi] \\
\textit{(small val)} & v & ::= r \mid w \mid v[\psi] \\
\textit{(heap val)} & h & ::= \langle w_1, \ldots, w_n \rangle \mid \mathtt{code}[\Delta]\langle \kappa \rangle \Gamma.I \\
\textit{(heaps)} & H & ::= \{l_1 \mapsto h_1, \ldots, l_n \mapsto h_n\} \\
\textit{(reg files)} & R & ::= \{r_1 \mapsto w_1, \ldots, r_n \mapsto w_n, \mathtt{sp} \mapsto S\} \\
\textit{(stacks)} & S & ::= nil \mid w :: S \\
\\
\textit{(instr)} & \iota & ::= \mathtt{add}\, r_d, r_s, v \mid \mathtt{ld}\, r_d, r_s(i) \mid \mathtt{st}\, r_d(i), r_s \\
 & & \quad \mid \mathtt{mov}\, r_d, v \mid \mathtt{bnz}\, r, v \mid \mathtt{salloc}\, i \mid \mathtt{sfree}\, i \\
 & & \quad \mid \mathtt{sld}\, r_d, \mathtt{sp}(i) \mid \mathtt{sst}\, \mathtt{sp}(i), r_s \mid \mathtt{raise}\, \kappa \\
\textit{(instr seq)} & I & ::= \iota; I \mid \mathtt{lower}\, w \mid \mathtt{jmp}\, v \mid \mathtt{halt}\, [\sigma] \\
\textit{(prog)} & P & ::= (H, R, I)_\kappa
\end{array}
$$

Figure 6. Syntax of TAL$_C$

4. TAL$_C$

4.1 Abstract Machine

Our language TAL$_C$ is designed to resemble TAL [18] for ease of understanding. We introduce some new constructs for confidentiality, and accommodate a stack following STAL [17] for supporting procedure calls. In the interest of simplicity, we maintain just enough features for demonstrating the certifying compilation of security types from our source language in Figure 1, removing from TAL and STAL features that are orthogonal to it.

We assume that security labels form a lattice $\mathcal{L}$. We use θ to range over elements of $\mathcal{L}$. We use $\bot$ and $\top$ as the bottom and top of the lattice, $\cup$ and $\cap$ as the lattice join and meet operations, and $\subseteq$ as the lattice ordering. The syntactic constructs of TAL$_C$ can be understood in three steps as follows.

Type constructs The top portion of Figure 6 presents the type constructs. Security contexts κ follow the idea of Section 3.2. An empty security context ($\bullet$) represents an program counter with the lowest security label. A concrete context ($\theta \triangleright w$) is made up of a security label θ (the current security level) and a postdominator w. The postdominator w has the syntax of a word value, but its use is restricted by the semantics to be eventually an instantiated code label, *i.e.,* the ending point of the current security level. The postdominator w could also be a variable α; this is useful for compiling procedures, which can be called in different contexts with different postdominators.

Pre-types (τ) reflect the normal types as seen in TAL, including integer types, tuple types, and code types. In comparison with TAL, our code type requires an extra security context (κ) as part of the interface. A type (σ) is either a pre-type tagged with a security label or a nonsense type (ns) for uninitialized stack slots. A stack type (Σ) is either a variable (ρ), or a (possibly empty) sequence of types. The variable context (Δ) is used for typing polymorphic code; it documents stack type variables (ρ) and postdominator variables (α). Stack types and postdominators are also generally referred to as type arguments ψ. Finally, heap types (Ψ) or register file types (Γ) are mappings from heap labels or registers to types; the `sp` in the register file represents the stack.

Judgment	Meaning
$\Delta \vdash \kappa$	κ is a valid context
$\Delta \vdash \tau$	τ is a valid pre-type
$\Delta \vdash \sigma$	σ is a valid type
$\Delta \vdash \Sigma$	Σ is a valid stack type
$\vdash \Psi$	Ψ is a valid heap type
$\Delta \vdash \Gamma$	Γ is a valid register file type
$\Delta \vdash \Gamma_1 \subseteq \Gamma_2$	Register file type Γ_1 weakens Γ_2
$\vdash H : \Psi$	Heap H has type Ψ
$\Psi \vdash S : \Sigma$	Stack S has type Σ
$\Psi \vdash R : \Gamma$	Register file R has type Γ
$\Psi \vdash h : \sigma$	Heap value h has type σ
$\Psi; \Delta \vdash w : \sigma$	Word value w has type σ
$\Psi; \Delta; \Gamma \vdash v : \sigma$	Small value v has type σ
$\Psi; \Delta; \Gamma; \kappa \vdash I$	I is a valid sequence of instructions
$\Psi; \Gamma \vdash P$	P is a valid program

Figure 8. TAL$_C$ typing judgments

Note that the type constructs provide two layers of security labels for a data pointer (*e.g.,* $\langle \mathtt{int}_{\theta_2} \rangle_{\theta_1}$; see Section 3.3) or a code pointer (*e.g.,* $(\forall[\circ].\langle \theta_2 \triangleright l \rangle\, \Gamma)_{\theta_1}$; see Section 3.4)—one ($\theta_1$) for the pointer itself, the other (θ_2) for the data or code being referenced.

Value constructs The middle portion of Figure 6 shows the value constructs. A word value w is either a variable, a heap label l, an immediate integer i, a nonsense value for an uninitialized stack slot, or another word value instantiated with a type argument. Small values v serve as the operands of some instructions; they are either registers r, word values w, or instantiated small values. Heap values h are either tuples or typed code sequences; they are the building blocks of the heap H. Note that a value does not carry a security label. This is consistent with the philosophy that a value is never intrinsically sensitive—it is sensitive only if it comes from a sensitive location [29], which is documented in the corresponding types (Ψ and Γ). Finally, a register file R stores the contents of all registers and the stack, where the stack is a (possibly empty) sequence of word values.

Code constructs Code constructs are given in the bottom portion of Figure 6. We retain a minimal set of instructions from TAL and STAL, and introduce two new instructions (`raise` κ and `lower` l) for manipulating the security context as discussed in Section 3. A program is the usual triple tagged with a security context. The security context facilitates the formal soundness proof, but does not affect the computation.

In the operational semantics (Figure 7), there are only two cases that modify the security context: `raise` κ' updates the security context to κ', and `lower` w picks up a new security context from the interface of the target code w. In all other cases, the security context remains the same, and the semantics is standard. It is easy to see that this operational semantics mimics the behavior of a real machine, and does not prohibit bad flows. One can obtain a conventional machine by removing the security contexts and `raise` κ instructions, and replacing `lower` w with `jmp` w.

4.2 Typing Rules

The static semantics consists of judgment forms summarized in Figure 8. A security context appears in the judgment of a valid instruction sequence. Heap and register file types are made explicit in the judgment of a valid program for facilitating the noninterference theorem. All other judgment forms closely resemble those of TAL and STAL.

$(H, R, I)_\kappa \longmapsto P$ where		
if $I =$	then $P =$	
$\texttt{add}\ r_d, r_s, v; I'$	$(H, R\{r_d \mapsto (i + i')\}, I')_\kappa$	where $R(r_s) = i$ and $\hat{R}(v) = i'$
$\texttt{ld}\ r_d, r_s(i); I'$	$(H, R\{r_d \mapsto w_i\}, I')_\kappa$	where $R(r_s) = l$ and $H(l) = \langle w_0, \ldots, w_{n-1}\rangle$ with $0 \le i < n$
$\texttt{mov}\ r_d, v; I'$	$(H, R\{r_d \mapsto \hat{R}(v)\}, I')_\kappa$	
$\texttt{bnz}\ r, v; I'$	$(H, R, I')_\kappa$ when $R(r) = 0$	
$\texttt{bnz}\ r, v; I'$	$(H, R, I''[\vec{\psi}/\Delta])_\kappa$ when $R(r) = i$	where $i \neq 0$ and $\hat{R}(v) = l[\vec{\psi}]$ and $H(l) = \texttt{code}[\Delta]\langle\kappa'\rangle\Gamma.I''$
$\texttt{st}\ r_d(i), r_s; I'$	$(H\{l \mapsto \langle w_0, \ldots, w_{i-1}, R(r_s), w_{i+1}, \ldots, w_{n-1}\rangle\}, R, I')_\kappa$	where $R(r_d) = l$ and $H(l) = \langle w_0, \ldots, w_{n-1}\rangle$ with $0 \le i < n$
$\texttt{salloc}\ i; I'$	$(H, R\{\texttt{sp} \mapsto \underbrace{ns :: \ldots :: ns}_{i} :: R(\texttt{sp})\}, I')_\kappa$	
$\texttt{sfree}\ i; I'$	$(H, R\{\texttt{sp} \mapsto S\}, I')_\kappa$	where $R(\texttt{sp}) = w_1 :: \ldots :: w_i :: S$
$\texttt{sld}\ r_d, \texttt{sp}(i); I'$	$(H, R\{r_d \mapsto w_i\}, I')_\kappa$	where $R(\texttt{sp}) = w_0 :: \ldots :: w_i :: S$ and $i \ge 0$
$\texttt{sst}\ \texttt{sp}(i), r_s; I'$	$(H, R\{\texttt{sp} \mapsto w_0 :: \ldots :: w_{i-1} :: R(r_s) :: S\}, I')_\kappa$	where $R(\texttt{sp}) = w_0 :: \ldots :: w_i :: S$ and $i \ge 0$
$\texttt{raise}\ \kappa'; I'$	$(H, R, I')_{\kappa'}$	
$\texttt{lower}\ w$	$(H, R, I'[\vec{\psi}/\Delta])_{\kappa'}$	where $w = l[\vec{\psi}]$ and $H(l) = \texttt{code}[\Delta]\langle\kappa'\rangle\Gamma.I'$
$\texttt{jmp}\ v$	$(H, R, I'[\vec{\psi}/\Delta])_\kappa$	where $\hat{R}(v) = l[\vec{\psi}]$ and $H(l) = \texttt{code}[\Delta]\langle\kappa'\rangle\Gamma.I'$

$$\text{where } \hat{R}(v) = \begin{cases} R(r) & \text{when } v = r \\ w & \text{when } v = w \\ \hat{R}(v')[\psi] & \text{when } v = v'[\psi] \end{cases}$$

Figure 7. Operational semantics of TAL$_C$

The typing rules are given in Figures 9 and 10. A type construct is valid (top six judgment forms in Figure 8) if all free type variables are documented in the type environment. Heap values and integers may have any security label. The types of heap labels and registers are as described in the heap type and the register file type respectively. All other rules for non-instructions are straightforward extensions of those in TAL and STAL.

We use $SL(\kappa)$ to refer to the security label component of κ. $SL(\bullet)$ is defined to be $\bot$. The typing rules for `add`, `ld` and `mov` instructions infer the security labels for the destination registers; they take into account the security labels of the source and target operands and the current security context.

The rule for `bnz` first checks that the guard register r is an integer and the target value v is a code label. It then checks that the current security context is high enough to cover the security levels of the guard (preventing flows through program structures; Section 3.2) and the target code (preventing flows through code pointers; Section 3.4). Lastly, the checks on the register file and the remainder instruction sequence make sure that both branches are secure to execute.

The rule for `st` concerns four security labels. The label of the target cell must be higher than or equal to those of the context (Section 3.2), the containing tuple (Section 3.3), and the source value (Section 3.1).

The rules for the stack instructions follow similar ideas. In essence, the stack can be viewed as an infinite number of registers. Instruction `salloc` or `sfree` add new slots to or remove existing slots from the slot, so the rules check the remainder instruction sequence under an updated stack type. The rule for instruction `sld` or `sst` can be understood following that of the `mov` instruction.

The rule for `raise` checks that the new security context is higher than the current one. Moreover, it looks at the postdominator w' of the new context, and makes sure that the security context at w' matches the current one. The remainder instruction sequence is checked under the new context.

Since the rule for `raise` already checked the validity of the ending label of a secured region, the task for ending the region is relatively simple. The rule for `lower` checks that its operand label matches that dictated by the security context. This guarantees that a secured region be enclosed within a `raise-lower` pair. The rule also makes sure that the code at w is safe to execute, which involves checking the security labels (Section 3.4) and the register file types.

The rule for `jmp` checks that the target code is safe to execute. Similar checks also appeared in the rule for `bnz`. In these two rules, the security context of the target code is always the same as the current one. This is because context changes are separated from conventional instructions in our system. For example, one may enclose high target code within `raise` and `lower` before calling it in a low context.

Finally, halting is valid only if the security context is empty, and the value in r_1 has the expected type σ.

Interested readers are referred to Appendix B for a simple example that demonstrates the use of security labels and contexts.

4.3 Soundness

TAL$_C$ enjoys conventional type safety (memory and control-flow safety), which can be established following the preservation and progress lemmas. The proofs of these lemmas are similar to those of TAL and STAL and omitted.

Lemma 1 (Preservation) If $\Psi; \Gamma \vdash P$ and $P \longmapsto P'$, then there exists Γ' such that $\Psi; \Gamma' \vdash P'$.

Lemma 2 (Progress) If $\Psi; \Gamma \vdash P$ then either:
(1) there exists P' such that $P \longmapsto P'$, or
(2) P is of the form $(H, R\{r_1 \mapsto w\}, \texttt{halt}\ [\sigma])_\bullet$ where $\vdash H : \Psi$ and $\Psi; \circ \vdash w : \sigma$.

Before presenting the noninterference theorem, we define the equivalence of two programs with respect to a security level θ.

Definition 1 (Heap Equivalence) $\Psi \vdash H_1 \approx_\theta H_2 \iff$ for every $l \in \mathrm{dom}(\Psi)$, if $\Psi(l) = \tau_{\theta'}$ and $\theta' \subseteq \theta$ then $H_1(l) = H_2(l)$.

Definition 2 (Stack Equivalence) $\Sigma \vdash S_1 \approx_\theta S_2 \iff$ for every slot $i \in \mathrm{dom}(\Sigma)$, if $\Sigma(i) = \tau_{\theta'}$ and $\theta' \subseteq \theta$ then $S_1(i) = S_2(i)$.

Definition 3 (Register File Equivalence) $\Gamma \vdash R_1 \approx_\theta R_2 \iff$ (1) $\Gamma(sp) \vdash R_1(sp) \approx_\theta R_2(sp)$, and (2) for every $r \in \mathrm{dom}(\Gamma)$, if $\Gamma(r) = \tau_{\theta'}$ and $\theta' \subseteq \theta$, then $R_1(r) = R_2(r)$.

$$\Delta \vdash \bullet \qquad \frac{freevar(w) \subseteq \Delta}{\Delta \vdash \theta \triangleright w} \qquad \Delta \vdash \mathtt{int}$$

$$\frac{\Delta \vdash \sigma_i}{\Delta \vdash \langle \sigma_1, \ldots, \sigma_n \rangle} \qquad \frac{\Delta \vdash \kappa \qquad \Delta \vdash \Gamma}{\Delta \vdash \forall[\Delta].\langle \kappa \rangle\, \Gamma}$$

$$\frac{\Delta \vdash \tau}{\Delta \vdash \tau_\theta} \qquad \Delta \vdash ns$$

$$\frac{\rho \in \Delta}{\Delta \vdash \rho} \qquad \Delta \vdash nil \qquad \frac{\Delta \vdash \sigma \qquad \Delta \vdash \Sigma}{\Delta \vdash \sigma :: \Sigma}$$

$$\frac{\circ \vdash \sigma_i}{\vdash \{l_1 : \sigma_1 \ldots l_n : \sigma_n\}} \qquad \frac{\Delta \vdash \sigma_i \qquad \Delta \vdash \Sigma}{\Delta \vdash \{r_1 : \sigma_1 \ldots r_n : \sigma_n, \mathtt{sp} : \Sigma\}}$$

$$\frac{\Delta \vdash \sigma_i \qquad \Delta \vdash \Sigma \qquad m \leq n}{\Delta \vdash \{r_1 : \sigma_1 \ldots r_m : \sigma_m, \mathtt{sp} : \Sigma\} \subseteq \{r_1 : \sigma_1 \ldots r_n : \sigma_n, \mathtt{sp} : \Sigma\}}$$

$$\frac{\vdash \Psi \qquad \Psi = \{l_1 : \sigma_1, \ldots l_n : \sigma_n\} \qquad \Psi \vdash h_i : \sigma_i}{\vdash \{l_1 \mapsto h_1, \ldots, l_n \mapsto h_n\} : \Psi}$$

$$\frac{\begin{array}{c}\Gamma = \{r_1 : \sigma_1, \ldots r_n : \sigma_n, \mathtt{sp} : \Sigma\} \\ \Psi \vdash w_i : \sigma_i \qquad \Psi \vdash S : \Sigma\end{array}}{\Psi \vdash \{r_1 \mapsto w_1, \ldots, r_n \mapsto w_n, \mathtt{sp} \mapsto S\} : \Gamma}$$

$$\frac{\Psi \vdash w_i : \sigma_i}{\Psi \vdash \langle w_1, \ldots, w_n \rangle : \langle \sigma_1, \ldots, \sigma_n \rangle_\theta}$$

$$\frac{\Delta \vdash \kappa \qquad \Delta \vdash \Gamma \qquad \Psi; \Delta; \Gamma; \kappa \vdash I}{\Psi \vdash \mathtt{code}[\Delta]\langle \kappa \rangle \Gamma.I : (\forall[\Delta].\langle \kappa \rangle\, \Gamma)_\theta}$$

$$\Psi; \Delta \vdash i : \mathtt{int}_\theta \qquad \Psi; \Delta \vdash ns : ns \qquad \frac{\Psi(l) = \sigma}{\Psi; \Delta \vdash l : \sigma}$$

$$\frac{\Delta \vdash \Sigma \qquad \Psi; \Delta \vdash w : \forall[\rho\Delta'].\langle \kappa \rangle\, \Gamma}{\Psi; \Delta \vdash w[\Sigma] : \forall[\Delta'].\langle \kappa[\Sigma/\rho] \rangle\, \Gamma[\Sigma/\rho]}$$

$$\frac{\Delta \vdash \Sigma \qquad \Psi; \Delta \vdash w : \forall[\alpha\Delta'].\langle \kappa \rangle\, \Gamma}{\Psi; \Delta \vdash w[w'] : \forall[\Delta'].\langle \kappa[w'/\alpha] \rangle\, \Gamma[w'/\alpha]}$$

$$\frac{\Gamma(r) = \sigma}{\Psi; \Delta; \Gamma \vdash r : \sigma} \qquad \frac{\Psi; \Delta \vdash w : \sigma}{\Psi; \Delta; \Gamma \vdash w : \sigma}$$

$$\frac{\Delta \vdash \Sigma \qquad \Psi; \Delta; \Gamma \vdash v : \forall[\rho\Delta'].\langle \kappa \rangle\, \Gamma'}{\Psi; \Delta; \Gamma \vdash v[\Sigma] : \forall[\Delta'].\langle \kappa[\Sigma/\rho] \rangle\, \Gamma'[\Sigma/\rho]}$$

$$\frac{\Delta \vdash \Sigma \qquad \Psi; \Delta; \Gamma \vdash v : \forall[\alpha\Delta'].\langle \kappa \rangle\, \Gamma'}{\Psi; \Delta; \Gamma \vdash v[w] : \forall[\Delta'].\langle \kappa[w/\alpha] \rangle\, \Gamma'[w/\alpha]}$$

$$\frac{\circ \vdash \kappa \qquad \vdash H : \Psi \qquad \Psi \vdash R : \Gamma \qquad \Psi; \circ; \Gamma; \kappa \vdash I}{\Psi; \Gamma \vdash (H, R, I)_\kappa}$$

Figure 9. TAL_C typing rules (non-instructions)

$$\frac{SL(\kappa) = \theta \qquad \Gamma(r_s) = \mathtt{int}_{\theta_1} \qquad \Psi; \Delta; \Gamma \vdash v : \mathtt{int}_{\theta_2} \qquad \Psi; \Delta; \Gamma\{r_d : \mathtt{int}_{\theta \cup \theta_1 \cup \theta_2}\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{add}\ r_d, r_s, v; I}$$

$$\frac{SL(\kappa) = \theta \qquad \Gamma(r_s) = \langle \sigma_1, \ldots, \sigma_n \rangle_{\theta_1} \qquad \sigma_i = \tau_{\theta_2} \qquad \Psi; \Delta; \Gamma\{r_d : \tau_{\theta \cup \theta_1 \cup \theta_2}\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{ld}\ r_d, r_s(i); I}$$

$$\frac{SL(\kappa) = \theta \qquad \Psi; \Gamma \vdash v : \tau_{\theta'} \qquad \Psi; \Delta; \Gamma\{r_d : \tau_{\theta \cup \theta'}\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{mov}\ r_d, v; I}$$

$$\frac{SL(\kappa) = \theta \qquad \Gamma(r) = \mathtt{int}_{\theta_1} \qquad \Psi; \Delta; \Gamma \vdash v : (\forall[\circ].\langle \kappa \rangle\, \Gamma')_{\theta_2} \qquad \theta_1 \cup \theta_2 \subseteq \theta \qquad \Delta \vdash \Gamma' \subseteq \Gamma \qquad \Psi; \Delta; \Gamma; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{bnz}\ r, v; I}$$

$$\frac{SL(\kappa) = \theta \qquad \Gamma(r_d) = \langle \sigma_1, \ldots, \sigma_n \rangle_{\theta_1} \qquad \sigma_i = \tau_{\theta'} \qquad \Gamma(r_s) = \tau_{\theta_2} \qquad \theta \cup \theta_1 \cup \theta_2 \subseteq \theta' \qquad \Psi; \Delta; \Gamma; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{st}\ r_d(i), r_s; I}$$

$$\frac{\Gamma(\mathtt{sp}) = \Sigma \qquad \Psi; \Delta; \Gamma\{\mathtt{sp} : \overbrace{ns :: \ldots :: ns}^{i} :: \Sigma\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{salloc}\ i; I}$$

$$\frac{\Gamma(\mathtt{sp}) = \sigma_1 :: \ldots :: \sigma_i :: \Sigma \qquad \Psi; \Delta; \Gamma\{\mathtt{sp} : \Sigma\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{sfree}\ i; I}$$

$$\frac{SL(\kappa) = \theta \qquad \Gamma(\mathtt{sp}) = \sigma_0 :: \ldots :: \sigma_i :: \Sigma \qquad \sigma_i = \tau_{\theta'} \qquad \Psi; \Delta; \Gamma\{r_d : \tau_{\theta \cup \theta'}\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{sld}\ r_d, \mathtt{sp}(i); I}$$

$$\frac{SL(\kappa) = \theta \qquad \Gamma(\mathtt{sp}) = \sigma_0 :: \ldots :: \sigma_i :: \Sigma \qquad \Gamma(r_s) = \tau_{\theta'} \qquad \Psi; \Delta; \Gamma\{\mathtt{sp} : \sigma_0 :: \ldots :: \sigma_{i-1} :: \tau_{\theta \cup \theta'} :: \Sigma\}; \kappa \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{sst}\ \mathtt{sp}(i), r_s; I}$$

$$\frac{\kappa = \theta \triangleright w \qquad \kappa' = \theta' \triangleright w' \qquad \theta \subseteq \theta' \qquad \Psi; \Delta \vdash w' : (\forall[\circ].\langle \kappa \rangle\, \Gamma')_{\theta_1} \qquad \Psi; \Delta; \Gamma; \kappa' \vdash I}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{raise}\ \kappa'; I}$$

$$\frac{\kappa = \theta \triangleright w \qquad \Psi; \Delta \vdash w : (\forall[\circ].\langle \kappa' \rangle\, \Gamma')_{\theta_1} \qquad \theta_1 \subseteq SL(\kappa') \qquad \Delta \vdash \Gamma' \subseteq \Gamma}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{lower}\ w}$$

$$\frac{SL(\kappa) = \theta \qquad \Psi; \Delta; \Gamma \vdash v : (\forall[\circ].\langle \kappa \rangle\, \Gamma')_{\theta_1} \qquad \theta_1 \subseteq \theta \qquad \Delta \vdash \Gamma' \subseteq \Gamma}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{jmp}\ v}$$

$$\frac{\kappa = \bullet \qquad \Delta \vdash \sigma \qquad \Gamma(r_1) = \sigma}{\Psi; \Delta; \Gamma; \kappa \vdash \mathtt{halt}\ [\sigma]}$$

Figure 10. Typing rules of TAL_C instructions

Definition 4 (Program Equivalence) $\Psi; \Gamma \vdash P_1 \approx_\theta P_2 \iff P_1 = (H_1, R_1, I_1)_{\kappa_1}$, $P_2 = (H_2, R_2, I_2)_{\kappa_2}$, $\Psi \vdash H_1 \approx_\theta H_2$, $\Gamma \vdash R_1 \approx_\theta R_2$, and either:
(1) κ_1=κ_2, $SL(\kappa_1) \subseteq \theta$, and $I_1 = I_2$, or
(2) $SL(\kappa_1) \not\subseteq \theta$, $SL(\kappa_2) \not\subseteq \theta$.

It is easy to see that the above relations are all reflexive, symmetrical, and transitive. Our noninterference theorem relates the executions of two equivalent programs that both start in a low security context (relative to the security level of concern). If both executions terminate, then the result programs must also be equivalent.

The idea of the proof is intuitive. Given a security level of concern, the executions can be phased into "low steps" and "high steps." It is easy to relate the two executions under a low step, because they involve the same instructions. Under a high step, the two executions are no longer in lock step. Recall that `raise` and `lower` mark the beginning and the end of a secured region. We relate the program states before the `raise` and after the `lower`, circumventing directly relating two executions under high steps.

We give the formal details in three lemmas and a noninterference theorem. Lemma 3 indicates that a security context in a high step can be changed only with `raise` or `lower`. Lemma 4 says that a terminating program must reduce to a step that discharges the current security context with a `lower`. Lemma 5 articulates the lock step relation between two equivalent programs in a low step. Theorem 1 of noninterference then follows. In the following, $\longmapsto^*$ represents the reflexive and transitive closure of $\longmapsto$. $\Sigma \succeq_\theta \Sigma'$ means that $\Sigma(i) = \Sigma'(i)$ for every i such that $\Sigma'(i) = \tau_{\theta'}$ and $\theta' \subseteq \theta$. $\Gamma \succeq_\theta \Gamma'$ means that $\Gamma(\mathtt{sp}) \succeq_\theta \Gamma'(\mathtt{sp})$ and $\Gamma(r) = \Gamma'(r)$ for every r such that $\Gamma'(r) = \tau_{\theta'}$ and $\theta' \subseteq \theta$. We use Q in addition to P to denote programs when comparing two executions. The proofs are given in Appendix A.

Lemma 3 (High Step) If $P = (H, R, I)_\kappa$, $SL(\kappa) \not\sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, then either: (1) there exists Γ_1 and $P_1 = (H_1, R_1, I_1)_\kappa$ such that $P \longmapsto P_1$, $\Psi; \Gamma_1 \vdash P_1$, $\Gamma \succeq_\theta \Gamma_1$, and $\Psi; \Gamma_1 \vdash P \approx_\theta P_1$, or (2) I is of the form $(\texttt{raise}\ \kappa'; I')$ or $(\texttt{lower}\ w)$.

Lemma 4 (Context Discharge) If $P = (H, R, I)_{\theta \triangleright w}$, $\theta \not\sqsubseteq \theta'$, $\Psi; \Gamma \vdash P$, $P \longmapsto^* (H_0, R_0, \texttt{halt}\ [\sigma])_\bullet$, then there exists Γ' and $P' = (H', R', \texttt{lower}\ w)_{\theta \triangleright w}$, such that $\Psi; \Gamma' \vdash P'$, $P \longmapsto^* P'$, $\Gamma \succeq_{\theta'} \Gamma'$, and $\Psi; \Gamma' \vdash P \approx_{\theta'} P'$.

Lemma 5 (Low Step) If $P = (H, R, I)_\kappa$, $SL(\kappa) \sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, $\Psi; \Gamma \vdash Q$, $\Psi; \Gamma \vdash P \approx_\theta Q$, $P \longmapsto P_1$, $Q \longmapsto Q_1$, then exists Γ_1 such that $\Psi; \Gamma_1 \vdash P_1$, $\Psi; \Gamma_1 \vdash Q_1$ and $\Psi; \Gamma_1 \vdash P_1 \approx_\theta Q_1$.

Theorem 1 (Noninterference) If $P = (H, R, I)_\kappa$, $SL(\kappa) \sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, $\Psi; \Gamma \vdash Q$, $\Psi; \Gamma \vdash P \approx_\theta Q$,
$P \longmapsto^* (H_p, R_p, \texttt{halt}\ [\sigma_p])_\bullet$, and
$Q \longmapsto^* (H_q, R_q, \texttt{halt}\ [\sigma_q])_\bullet$, then exists Γ' such that
$\Psi; \Gamma' \vdash (H_p, R_p, \texttt{halt}\ [\sigma_p])_\bullet \approx_\theta (H_q, R_q, \texttt{halt}\ [\sigma_q])_\bullet$.

5. Certifying Compilation

Certifying compilation for a realistic language typically involves a complex sequence of transformations, including CPS and closure conversion, heap allocation, and code generation [18, 15]. In this paper, we choose the simple security-type system of Figure 1 as our source language. This allows a concise presentation, yet suffices in demonstrating a main contribution: the separation of security-context operations (`raise` and `lower`) from conventional instructions and mechanisms (*e.g.*, stack convention for procedure calls).

The low-high security hierarchy of Figure 1 defines a simple lattice consisting of two elements: $\bot$ and $\top$. We use $|\texttt{t}|$ to denote the translation of source type `t` in TAL$_C$: $|\texttt{low}| \equiv \texttt{int}_\bot$ and $|\texttt{high}| \equiv \texttt{int}_\top$. We also translate the procedure types from the source language into TAL$_C$ as follows:

$$|\langle \texttt{pc} \rangle (\texttt{t}_1, \ldots, \texttt{t}_n) \to \texttt{void}| = (\forall[\Delta].\langle\kappa\rangle\ \{\texttt{sp} : \Sigma\})_\bot$$
$$\text{where } (\Delta, \kappa) = \begin{cases} (\rho\circ, \bullet) & \text{if } \texttt{pc} = \texttt{low} \\ (\alpha\rho\circ, \top \triangleright \alpha) & \text{if } \texttt{pc} = \texttt{high} \end{cases}$$
$$\text{and } \Sigma = (\forall[\Delta].\langle\kappa\rangle\ \{\texttt{sp} : \rho\})_\bot :: \langle|\texttt{t}_1|\rangle_\bot :: \ldots :: \langle|\texttt{t}_n|\rangle_\bot :: \rho$$

This procedure type translation assumes a calling convention where the caller pushes a return pointer and the location of the arguments (implementing the call-by-reference semantics of the source language) onto the stack, and the callee deallocates the current stack frame upon return. The stack type Σ refers to a variable ρ because the procedure may be called under different stacks, as long as the current stack frame is as expected. The security context κ is empty if `pc` is `low`, or $\top \triangleright \alpha$ if `pc` is `high`. Postdominator variable α is used because the procedure may be called in security contexts with different postdominators. The type environment Δ simply collects all the needed type variables.

We assume that the program translation starts in a heap H_0 and a heap type Ψ_0 which satisfy $\vdash H_0 : \Psi_0$ and contain entries for all the variables and procedures of the source program. For any source variable `v` that $\Phi(\texttt{v}) = \texttt{t}$, there exists a location $l_\texttt{v}$ in the heap such that $\Psi(l_\texttt{v}) = \langle|\texttt{t}|\rangle_\bot$. For any source procedure `f` that $\Phi(\texttt{f}) = \langle\texttt{pc}\rangle(\texttt{t}_1, \ldots, \texttt{t}_n) \to \texttt{void}$, there exists a location $l_\texttt{f}$ in the heap such that $\Psi(l_\texttt{f}) = |\langle\texttt{pc}\rangle(\texttt{t}_1, \ldots, \texttt{t}_n) \to \texttt{void}|$. We use $\Phi \sim \Psi$ to refer to this correspondence.

The above heap H_0 can be constructed with dummy slots for the procedures—the code in there simply jumps to itself. This suffices for typing the initial heap, thus facilitating the type-preservation proof. It creates locations for all source procedures and allows the translation of the actual code to refer to them.

[TREconst] $$|\texttt{i}| = \texttt{mov}\ r, i \,||\, r$$

[TREvar] $$|\texttt{v}| = \texttt{mov}\ r, l_\texttt{v}; \texttt{ld}\ r', r(0) \,||\, r'$$

[TREarg] $$|\texttt{x}_i| = \texttt{sld}\ r, \texttt{sp}(i); \texttt{ld}\ r', r(0) \,||\, r'$$

[TREadd] $$\frac{|\texttt{E}| = \vec{\iota} \,||\, r \qquad |\texttt{E}'| = \vec{\iota'} \,||\, r' \qquad \vec{\iota'} \text{ does not use } r}{|\texttt{E} + \texttt{E}'| = \vec{\iota}, \vec{\iota'}; \texttt{add}\ r'', r, r' \,||\, r''}$$

Figure 11. Expression translation

The translation details are given in Figures 11, 12 and 13, based on the structure of the typing derivation of the source program. Which translation rule to apply is determined by the last typing rule used to check the source construct (program, procedure, or command). We use `TD` to denote (possibly multiple) typing derivations.

We define expression translation of the form $|\texttt{E}| = \vec{\iota} \,||\, r$ in Figure 11. The instruction vector $\vec{\iota}$ computes the value of `E` and the result is put in the register r. For a global variable, the value is loaded from the heap using its corresponding heap label. For a procedure argument, the location of the actual entity is loaded from the stack, and the value is then loaded from the heap.

In Figure 12, when translating a program (Rule [TRP1]), we translate all the procedure declarations, add halting code as the ending point of the program, and proceed to translate the main command. The result triple contains the updated heap type and heap, and a starting label l which leads to the starting point of the program. Procedure translation (Rule [TRF1]) takes care of part of the calling convention. It adds epilogue code that loads the return pointer, deallocates the current stack frame and transfers the control to the return pointer. It then resorts to command translation to translate the procedure body, providing the label to the epilogue code as the ending point of the procedure body.

In Figure 13, we define command translation of the form

$$\left| \frac{\texttt{TD}}{[\texttt{pc}] \vdash \texttt{C}} \right| \left[\begin{array}{l} \Psi \\ H \\ l_{start}; l_{end}; \Delta; \kappa; \Sigma \end{array} \right] = \left[\begin{array}{l} \Psi' \\ H' \end{array} \right].$$

This command translation takes 7 arguments: a code heap type (Ψ), a code heap (H), starting and ending labels (l_{start} and l_{end}) for the computation of `C`, a type environment (Δ), a security context (κ), and a stack type (Σ). It generates the extended code heap type (Ψ') and code heap (H'). Unsurprisingly, this translation appears complex, because it provides a formal model of a certifying compiler. Nonetheless, it is easy to follow if we remember some invariants maintained by the translation:

- H is well-typed under Ψ and contains entries for all source variables and procedures;
- Ψ and H already contain the continuation code labeled l_{end};
- The new code labeled l_{start} will be put into Ψ' and H';
- The security context κ must match `pc`;
- The stack type Σ contains entries for all procedure arguments, if the command being compiled is in the body of a procedure;
- The environment Δ contains all free type variables in κ and Σ.

Most of the command translation rules simply put Δ, κ and Σ in place for the generated code types, and further propagate them to the translation of sub-components. The only rule that non-trivially manipulates the security context is Rule [TRC4]—when a subsumption rule is used for typing a source command, the translation generates code that is enclosed in a `raise-lower` pair. The translation of the sub-component is carried out in an updated heap with a new ending label l_1. The code at l_1 restores the security context and transfers the control to the given ending label l'. After

$$\text{[TRP1]}\quad \frac{\left|\frac{\texttt{TD}_i}{\Phi \vdash \texttt{F}_i}\right| \begin{bmatrix}\Psi_{i-1}\\ H_{i-1}\end{bmatrix} = \begin{bmatrix}\Psi_i\\ H_i\end{bmatrix} \quad \forall i \in \{1\ldots n\} \qquad l_{halt} \text{ is a fresh label}}{\left|\frac{\texttt{TD}}{\Phi;[\texttt{low}] \vdash \texttt{C}}\right| \begin{bmatrix}\Psi_n\{l_{halt} : (\forall[\circ].\langle\bullet\rangle\{\texttt{sp} : nil\})_\perp\}\\ H_n\{l_{halt} \mapsto \texttt{code}[\circ]\langle\bullet\rangle\{\texttt{sp} : nil\}.\texttt{mov}\ r_1, 1; \texttt{halt}\ [\texttt{int}_\perp]\}\\ l; l_{halt}; \circ; \bullet; nil\end{bmatrix} = \begin{bmatrix}\Psi\\ H\end{bmatrix}}{\left|\frac{\frac{\texttt{TD}_i}{\Phi \vdash \texttt{F}_i} \quad \forall i \in \{1\ldots n\} \qquad \frac{\texttt{TD}}{\Phi;[\texttt{low}] \vdash \texttt{C}} \quad \ldots}{\Phi \vdash \{\texttt{F}_1; \ldots; \texttt{F}_n; \texttt{C}\}}\right| \begin{bmatrix}\Psi_0\\ H_0\end{bmatrix} = \begin{bmatrix}\Psi\\ H; l\end{bmatrix}}$$

$$\left|\frac{\texttt{TD}}{\texttt{x}_1:\texttt{t}_1, \ldots, \texttt{x}_n:\texttt{t}_n, \Phi; [\texttt{pc}] \vdash \texttt{C}}\right| \begin{bmatrix}\Psi\{l : (\forall[\Delta].\langle\kappa\rangle\{\texttt{sp} : \Sigma\})_\perp\}\\ H\{l \mapsto \texttt{code}[\Delta]\langle\kappa\rangle\{\texttt{sp} : \Sigma\}.\\ \qquad \texttt{sld}\ r, \texttt{sp}(0); \texttt{sfree}\ (n{+}1); \texttt{jmp}\ r\}\\ l_{\texttt{f}}; l; \Delta; \kappa; \Sigma\end{bmatrix} = \begin{bmatrix}\Psi'\\ H'\end{bmatrix}$$

where $(\Delta, \kappa) = \begin{cases}(\rho\circ, \bullet) & \text{if } \texttt{pc} = \texttt{low}\\ (\alpha\rho\circ, \top \triangleright \alpha) & \text{if } \texttt{pc} = \texttt{high}\end{cases}$ l is a fresh label

$$\text{[TRF1]}\quad \frac{\Sigma = (\forall[\Delta].\langle\kappa\rangle\{\texttt{sp} : \rho\})_\perp :: \langle|\texttt{t}_1|\rangle_\perp :: \ldots :: \langle|\texttt{t}_n|\rangle_\perp :: \rho}{\left|\frac{\texttt{TD}}{\frac{\texttt{x}_1:\texttt{t}_1, \ldots, \texttt{x}_n:\texttt{t}_n, \Phi; [\texttt{pc}] \vdash \texttt{C}}{\Phi \vdash \texttt{f}\langle\texttt{pc}\rangle(\texttt{x}_1:\texttt{t}_1, \ldots, \texttt{x}_n:\texttt{t}_n)\{\texttt{C}\}}}\right| \begin{bmatrix}\Psi\\ H\end{bmatrix} = \begin{bmatrix}\Psi'\\ H'\end{bmatrix}}$$

Figure 12. Program and procedure declaration translation

the translation of the sub-component, code is added at the starting label l to raise the security context to the expected level.

Procedure call translation is given as Rule [TRC7]. It creates "prologue" code that allocates a stack frame, pushes the return pointer and the arguments onto the stack, and jumps to the procedure label. Note that the corresponding epilogue code is generated by the procedure declaration translation in Rule [TRF1].

The translation of while-loops is also interesting (Rule [TRC6]). When translating the loop body, we need to prepare the continuation block, which happens to be the code for the loop test. We make use of a dummy block labeled l to serve as the continuation block when translating the body C. This block is introduced for maintaining the above invariants. It facilitates the type-preservation proof of the translation. After the translation of the loop body, this dummy block is replaced with the actual code that implements the loop test, as shown on the bottom right side of Rule [TRC6].

Lemma 6 (Expression Translation) If $\Phi \sim \Psi$, $\Phi \vdash \texttt{E} : \texttt{t}$, $|\texttt{E}| = \vec{\imath}\,||\, r$, and $\Psi; \Delta; \{r : |\texttt{t}|, \texttt{sp} : \Sigma\}; \kappa \vdash I$, then $\Psi; \Delta; \{\texttt{sp} : \Sigma\}; \kappa \vdash \vec{\imath}; I$.

Lemma 7 (Command Translation) If $\Phi \sim \Psi$, $\Phi; [\texttt{pc}] \vdash \texttt{C}$, $\left|\frac{\texttt{TD}}{\Phi; [\texttt{pc}] \vdash \texttt{C}}\right| \begin{bmatrix}\Psi\\ H\\ l_{start}; l_{end}; \Delta; \kappa; \Sigma\end{bmatrix} = \begin{bmatrix}\Psi'\\ H'\end{bmatrix}$, $\Psi(l_{end}) = (\forall[\Delta].\langle\kappa\rangle\{\texttt{sp} : \Sigma\})_\perp$, $SL(\kappa) = |\texttt{pc}|$, $\vdash H : \Psi$, then $\Phi \sim \Psi'$, $\vdash H' : \Psi'$ and $\Psi'; \Delta \vdash l_{start} : (\forall[\Delta].\langle\kappa\rangle\{\texttt{sp} : \Sigma\})_\perp$.

The proofs for the above two lemmas are straightforward by structural induction on the derivation of the translation. Type preservation of procedure translation can be derived from Lemma 7 based on Rule [TRF1]. Type preservation of program translation then follows based on Rule [TRP1].

Lemma 8 (Procedure Translation) If $\Phi \sim \Psi$, $\Phi \vdash \texttt{F}$, $\vdash H : \Psi$, $\left|\frac{\texttt{TD}}{\Phi \vdash \texttt{F}}\right| \begin{bmatrix}\Psi\\ H\end{bmatrix} = \begin{bmatrix}\Psi'\\ H'\end{bmatrix}$, then $\Phi \sim \Psi'$ and $\vdash H' : \Psi'$.

Theorem 2 (Program Translation) If $\Phi \sim \Psi_0$, $\Phi \vdash \texttt{P}$, $\vdash H_0 : \Psi_0$, $\left|\frac{\texttt{TD}}{\Phi \vdash \texttt{P}}\right| \begin{bmatrix}\Psi_0\\ H_0\end{bmatrix} = \begin{bmatrix}\Psi\\ H; l\end{bmatrix}$, then $\Phi \sim \Psi$ and $\Psi; \{\texttt{sp} : nil\} \vdash (H, \{\texttt{sp} : nil\}, \texttt{jmp}\ l)_\bullet$.

6. Discussions

Linear Continuations Zdancewic and Myers [33] introduced a notion of ordered linear continuations to facilitate the information-flow analysis at a low level (we use ZM to refer to their system). An important requirement of such analysis is that one needs to allow a high-security conditional to be surrounded by low-security computation. In ZM, before the conditional statement, a linear continuation is created to capture the computation after the conditional. Such a linear continuation must be called exactly once at the end of either branch of the conditional. Furthermore, the linear continuation records the security context in which it is created, allowing the security context to be reset properly when the branches meet.

As a higher-order analog to postdominators in a control-flow graph, ordered linear continuations enforce a stack discipline that allows security contexts to be reset at the join points of program branches. The static semantics ensures that the linear continuations are properly nested, and at any time only the top continuation on the (virtual) continuation stack is available. The linearity is enforced because the continuation is essentially popped off the stack when used. In particular, every value in ZM is tagged with a security label. The operational semantics keeps track of the security context during the execution, and ensures that security labels of the values are propagated correctly.

It may help to view our solution as an adaptation of linear continuations for the RISC architecture (we emphasize that there is not a loss of expressiveness; interested readers are referred to Appendix C for some details). A postdominator of program branches is essentially expressed as a static code label. The security operations `raise` and `lower` correspond to the creation and elimination of linear continuations. At any program point, our static semantics keeps track of only the top element of the (virtual) continuation stack. The typing rule for `raise` ensures that the security context at the postdominator matches the current one, thus enforcing the stack discipline.

[TRC1]
$$\frac{|\mathtt{E}| = \vec{\iota}\,||\,r}{\left|\dfrac{\Phi(\mathtt{V}) = \mathtt{high}}{\Phi;[\mathtt{pc}] \vdash \mathtt{V} := \mathtt{E}}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi\{l : (\forall[\Delta].\langle\kappa\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H\{l \mapsto \mathtt{code}[\Delta]\langle\kappa\rangle\{\mathtt{sp} : \Sigma\}.\vec{\iota}; \mathtt{mov}\ r', l_{\mathrm{v}}; \mathtt{st}\ r'(0), r; \mathtt{jmp}\ l'[\Delta]\}\end{array}\right]}$$

[TRC2]
$$\frac{|\mathtt{E}| = \vec{\iota}\,||\,r}{\left|\dfrac{\Phi(\mathtt{V}) = \mathtt{low} \quad \Phi \vdash \mathtt{E} : \mathtt{low}}{\Phi;[\mathtt{low}] \vdash \mathtt{V} := \mathtt{E}}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \bullet; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi\{l : (\forall[\Delta].\langle\bullet\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H\{l \mapsto \mathtt{code}[\Delta]\langle\bullet\rangle\{\mathtt{sp} : \Sigma\}.\vec{\iota}; \mathtt{mov}\ r', l_1; \mathtt{st}\ r'(0), r; \mathtt{jmp}\ l'[\Delta]\}\end{array}\right]}$$

[TRC3]
$$\frac{\begin{array}{l}|\mathtt{E}| = \vec{\iota}\,||\,r \qquad l_1, l_2 \text{ are fresh labels}\\ \left|\dfrac{\mathtt{TD}_1}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1}\right| \left[\begin{array}{l}\Psi\\ H\\ l_1; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_1\\ H_1\end{array}\right] \qquad \left|\dfrac{\mathtt{TD}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}\right| \left[\begin{array}{l}\Psi_1\\ H_1\\ l_2; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_2\\ H_2\end{array}\right]\end{array}}{\left|\dfrac{\Phi \vdash \mathtt{E} : \mathtt{pc} \quad \dfrac{\mathtt{TD}_1}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1} \quad \dfrac{\mathtt{TD}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}}{\Phi;[\mathtt{pc}] \vdash \mathtt{if}\ \mathtt{E}\ \mathtt{then}\ \mathtt{C}_1\ \mathtt{else}\ \mathtt{C}_2}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_2\{l : (\forall[\Delta].\langle\kappa\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H_2\{l \mapsto \mathtt{code}[\Delta]\langle\kappa\rangle\{\mathtt{sp} : \Sigma\}.\vec{\iota}; \mathtt{bnz}\ r, l_1[\Delta]; \mathtt{jmp}\ l_2[\Delta]\}\end{array}\right]}$$

[TRC4]
$$\frac{\left|\dfrac{\mathtt{TD}}{\Phi;[\mathtt{high}] \vdash \mathtt{C}}\right| \left[\begin{array}{l}\Psi\{l_1 : (\forall[\Delta].\langle\top \triangleright l'[\Delta]\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H\{l_1 \mapsto \mathtt{code}[\Delta]\langle\top \triangleright l'[\Delta]\rangle\{\mathtt{sp} : \Sigma\}.\mathtt{lower}\ l'[\Delta]\}\\ l_0; l_1; \Delta; \top \triangleright l'[\Delta]; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi'\\ H'\end{array}\right] \qquad l_0, l_1 \text{ are fresh labels}}{\left|\dfrac{\dfrac{\mathtt{TD}}{\Phi;[\mathtt{high}] \vdash \mathtt{C}}}{\Phi;[\mathtt{low}] \vdash \mathtt{C}}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \bullet; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi'\{l : (\forall[\Delta].\langle\bullet\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H'\{l \mapsto \mathtt{code}[\Delta]\langle\bullet\rangle\{\mathtt{sp} : \Sigma\}.\mathtt{raise}\ \top \triangleright l'[\Delta]; \mathtt{jmp}\ l_0[\Delta]\}\end{array}\right]}$$

[TRC5]
$$\frac{\begin{array}{l}l_1 \text{ is a fresh label}\\ \left|\dfrac{\mathtt{TD}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}\right| \left[\begin{array}{l}\Psi\\ H\\ l_1; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_1\\ H_1\end{array}\right] \qquad \left|\dfrac{\mathtt{TD}_1}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1}\right| \left[\begin{array}{l}\Psi_1\\ H_1\\ l; l_1; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_2\\ H_2\end{array}\right]\end{array}}{\left|\dfrac{\dfrac{\mathtt{TD}_1}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1} \quad \dfrac{\mathtt{TD}_2}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_2}}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}_1; \mathtt{C}_2}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi_2\\ H_2\end{array}\right]}$$

[TRC6]
$$\frac{|\mathtt{E}| = \vec{\iota}\,||\,r \qquad \left|\dfrac{\mathtt{TD}}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}}\right| \left[\begin{array}{l}\Psi\{l : (\forall[\Delta].\langle\kappa\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H\{l \mapsto \mathtt{code}[\Delta]\langle\kappa\rangle\{\mathtt{sp} : \Sigma\}.\mathtt{jmp}\ l[\Delta]\}\\ l_1; l; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi'\\ H'\end{array}\right]}{\left|\dfrac{\Phi \vdash \mathtt{E} : \mathtt{pc} \quad \dfrac{\mathtt{TD}}{\Phi;[\mathtt{pc}] \vdash \mathtt{C}}}{\Phi;[\mathtt{pc}] \vdash \mathtt{while}\ \mathtt{E}\ \mathtt{do}\ \mathtt{C}}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi'\{l : (\forall[\Delta].\langle\kappa\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H'\{l \mapsto \mathtt{code}[\Delta]\langle\kappa\rangle\{\mathtt{sp} : \Sigma\}.\vec{\iota}; \mathtt{bnz}\ r, l_1[\Delta]; \mathtt{jmp}\ l'[\Delta]\}\end{array}\right]}$$

[TRC7]
$$\frac{\begin{array}{l}|\mathtt{V}_i| = \vec{\iota_i}\,||\,r_i \text{ where } \vec{\iota_i} \text{ does not use } r_j \text{ if } j < i \quad \forall i \in \{1 \ldots n\}\\ \Psi' = \Psi\{l : (\forall[\Delta].\langle\kappa\rangle\,\{\mathtt{sp} : \Sigma\})_\perp\}\\ H' = \Psi\{l \mapsto \mathtt{code}[\Delta]\langle\kappa\rangle\{\mathtt{sp} : \Sigma\}.\vec{\iota_1}; \ldots \vec{\iota_n}; \mathtt{salloc}\ (n+1); \mathtt{sst}\ \mathtt{sp}(0), l'[\vec{\psi}];\\ \qquad\qquad \mathtt{sst}\ \mathtt{sp}(1), r_1; \ldots \mathtt{sst}\ \mathtt{sp}(n), r_n; \mathtt{jmp}\ l_{\mathtt{f}}[\vec{\psi}]\} \qquad \text{where } \vec{\psi} = \begin{cases}\Sigma & \text{if } \kappa = \bullet\\ w\Sigma & \text{if } \kappa = \top \triangleright w\end{cases}\end{array}}{\left|\dfrac{\Phi(\mathtt{f}) = \langle\mathtt{pc}\rangle(\mathtt{t}_1, \ldots, \mathtt{t}_n) \to \mathtt{void} \qquad \dfrac{\mathtt{TD}_i}{\Phi \vdash \mathtt{V}_i : \mathtt{t}_i} \quad \forall i \in \{1 \ldots n\}}{\Phi;[\mathtt{pc}] \vdash \mathtt{f}(\mathtt{V}_1, \ldots, \mathtt{V}_n)}\right| \left[\begin{array}{l}\Psi\\ H\\ l; l'; \Delta; \kappa; \Sigma\end{array}\right] = \left[\begin{array}{l}\Psi'\\ H'\end{array}\right]}$$

Figure 13. Command translation

```
int double(x:int) { x=x*2; } ...
if h<10 then double(h);
double(l); ...
```

Figure 14. Security-polymorphic function

We wish to point out, nonetheless, that such an adaptation yields a simple, practical and well-grounded solution to the identified problem of information-flow analysis for assembly code. In particular, it bridges the gap between the functional abstraction of linear continuations and the raw assembly code running on actual machines. In comparison with ZM, our system TAL$_C$ models the use of registers and assembly instructions, and hence is closer to the actual RISC architecture. We do not attach security labels to values; this makes it trivial to see that security annotations do not affect computation. In fact, the enforcement of noninterference in TAL$_C$ is cleanly separated from normal program execution.[1] It is also obvious that security operations in TAL$_C$ are orthogonal from conventional instructions (*e.g.*, branching and jumping) and mechanisms (*e.g.*, call stack), which allows our approach to be carried further with other language extensions. Consequently, we consider TAL$_C$ as a good first step toward a scaled-up typed assembly language for noninterference.

SIF SIF [16] is developed independently from TAL$_C$. These two systems are similar in spirit—both use static types for information-flow analysis. However, SIF is based on a minimal language where relatively simple annotations, namely a stack of static code labels, suffice. In a more realistic language, a single function (even if monomorphic with respect to security levels) can be called at different program points. The security contexts of these program points may be different with respect to (1) the postdominator of the current context (SIF tracks this with the top stack element), and (2) the "enclosing contexts" (SIF tracks these with the stack tail). Since the label stack of SIF is made up of static code labels, one cannot reuse the same code at different program points with different contexts.

TAL$_C$ only maintains the current security context at any program point, and we show that it suffices for establishing noninterference. With such a treatment, the code types are naturally polymorphic with respect to enclosing contexts. We also allow postdominators to be polymorphic. The certifying compilation scheme further demonstrates that TAL$_C$ is expressive enough for supporting the source language.

7. Extensions and Future Work

Orthogonal features For ease of understanding, TAL$_C$ focuses on a minimal set of language features. Nonetheless, polymorphic and existential types, as seen in TAL, are orthogonal and can be introduced with little difficulty. Furthermore, since TAL$_C$ is compatible with TAL, it is also possible to accommodate other features of the TAL family. For instance, alias types [26] may provide a more accurate alias analysis, improving the current conservative approach that considers every pointer as a potential alias. In the following, we will also discuss the use of singleton types [32].

Security polymorphism TAL$_C$ relies on a security context $\theta \triangleright w$ to identify the current security level θ and its ending point w. It is monomorphic with respect to security, because the security level of a code block is fixed. In practice, security-polymorphic code can also be useful.

Figure 14 gives an example. The function `double` can be invoked with either low or high input. It is safe to invoke `double` in a context if only the security level of the input matches that of the context. In a security polymorphic TAL$_C$-like type system, `double` can be given the type

$$(\forall[\theta,\alpha].\langle\theta \triangleright \alpha\rangle\{r_1 : \mathtt{int}_\theta, r_0 : (\forall[].\langle\theta \triangleright \alpha\rangle\{r_1 : \mathtt{int}_\theta\})_\perp\})_\perp.$$

Here r_1 is the argument register, r_0 stores the return pointer, and the meta-variable θ is reused as a variable.

It is straightforward to support this kind of polymorphism. In fact, most of the required constructs are already present in TAL$_C$. We omitted such polymorphism simply because it complicates the presentation without providing additional insights. Nonetheless, the expressiveness of such polymorphism is still limited. Since the label α is not known until instantiated, the code of `double` has no knowledge about α. Hence the security context $\theta \triangleright \alpha$ cannot be discharged within the body of `double`.

It is not obvious why one would wish to discharge the security context within a polymorphic function. Indeed, it is always possible to wrap a function call inside a secured region by symmetric `raise` and `lower` operations from the caller's side. However, the asymmetric discharging of security context may be desirable for *certifying optimization*. For instance, in Figure 14, `double` is called as the last statement of the body of a high conditional. In this case, directly discharging the security context when `double` returns would remove a superfluous `lower` from the caller's side. Such a discharging requires `lower` to operate on small values—since the return label is not statically fixed, it must be passed in through a register.

It may require singleton and intersection types to support such a `lower` operation. For example, a `double` function that discharges its security context can have type

$$\left(\forall[\theta,\alpha].\langle\theta \triangleright \alpha\rangle \left\{\begin{array}{l} r_1 : \mathtt{int}_\theta, \\ r_0 : \mathtt{sint}(\alpha)_\perp \wedge (\forall[].\langle\bullet\rangle\{r_1 : \mathtt{int}_\theta\})_\perp \end{array}\right\}\right)_\perp.$$

At the end of the function, `lower` r_0 discharges the security context and transfers the control to the return code. For type checking, the singleton integer type $\mathtt{sint}(\alpha)$ matches the register r_0 with the label in the security context, and the code type ensures that the control flow to the return point is safe.

Full erasure With the powerful type constructs above, one can achieve a full erasure for the `lower` operation. Instead of treating `lower` as an instruction, one can treat it as a transformation on small values. This is in spirit similar to the *pack* operation of existential types in TAL. Such a `lower` transformation bridges the gap between the current security context and the security level of the target label. The actual control flow transfer is then completed with a conventional jump instruction (*e.g.*, `jmp` (`lower` r_0)).

One can also achieve a full erasure for `lower` even without singleton types. The idea is to separate the jump instruction into direct jump and indirect jump. This is also consistent with real machine architectures. The `lower` operation transforms word values (eventually, direct labels). Lowered labels, similar to packed values, may serve as the operand of direct jump. Indirect jump, on the other hand, takes normal small values. This is expressive enough for certifying compilation, yet may not be sufficient for certifying optimization as discussed above.

Other future work It is a challenging task to study how the features above yield a system expressive enough for certifying optimization. In TAL$_C$, `lower` erases to a direct jump, hence consecutive lower operations result in superfluous jumps. Ideally, these should be combined into a single jump whose operand is a nested lowered value. Similarly, it is also desirable to combine `lower` with an adjacent jump instruction. In practice, certifying optimization are sometimes considered for conventional type safety [9].

[1] The extra subscript of security context in a program P is only for facilitating the noninterference proof; it can be completely ignored for computation.

A security-type preserving translation for a full-fledged source language is another challenging task. The formal translation and type-preservation theorem in this paper are based on a concise source language for demonstrative purposes. Practical embodiment requires much further work. Existing work on type-preserving translation [18, 15] and high-level information-flow analysis [23] may shed light on the support of more advanced language features.

8. Conclusion

We have presented a language TAL_C for enforcing data confidentiality in assembly code. The main idea is to use type annotations to restore high-level abstractions that are crucial to information-flow analysis. In TAL_C, operations related to security are kept orthogonal from other language features. As a result, it is possible to accommodate existing results on low-level verification, such as the TAL family. We have also presented a translation from a high-level security language with first-order procedures to TAL_C. A soundness theorem shows that the translation preserves security types. We consider this as a useful step toward a certifying compiler for noninterference.

Acknowledgments

We wish to thank Eduardo Bonelli, Adriana Compagnoni, Ricardo Medel, Greg Morrisett, Steve Zdancewic and the anonymous referees for helpful comments on previous drafts of this paper.

References

[1] M. Abadi, A. Banerjee, H. Heintze, and J. G. Riecke. A core calculus of dependency. In *Proc. 26th ACM Symposium on Principles of Programming Languages*, pages 147–160, San Antonio, TX, Jan. 1999.

[2] J. Agat. Transforming out timing leaks. In *Proc. 27th ACM Symposium on Principles of Programming Languages*, pages 40–53, Boston, MA, Jan. 2000.

[3] J. Agat. *Type Based Techniques for Covert Channel Elimination and Register Allocation*. PhD thesis, Chalmers University of Technology and Gothenburg University, Gothenburg, Sweden, Dec. 2000.

[4] M. Avvenuti, C. Bernardeschi, and F. Francesco. Java bytecode verification for secure information flow. *ACM SIGPLAN Notices*, 38(12):20–27, Dec. 2003.

[5] T. Ball. What's in a region? Or computing control dependence regions in near-linear time for reducible control flow. *ACM Letters on Programming Languages and Systems*, 2(1–4):1–16, Mar.–Dec. 1993.

[6] A. Banerjee and D. A. Naumann. Secure information flow and pointer confinement in a Java-like language. In *Proc. 15th IEEE Computer Security Foundations Workshop*, pages 253–267, June 2002.

[7] G. Barthe, A. Basu, and T. Rezk. Security types preserving compilation. In *Proc. 5th International Conference on Verification, Model Checking and Abstract Interpretation*, volume 2937 of *LNCS*, pages 2–15, Venice, Italy, Jan. 2004.

[8] E. Bonelli, A. Compagnoni, and R. Medel. SIFTAL: A typed assembly language for secure information flow analysis. Technical report, Stevens Institute of Technology, Hoboken, NJ, July 2004.

[9] J. Chen, D. Wu, A. W. Appel, and H. Fang. A provably sound TAL for back-end optimization. In *Proc. 2003 ACM Conference on Programming Language Design and Implementation*, pages 208–219, San Diego, CA, June 2003.

[10] D. E. R. Denning. *Cryptography and Data Security*. Addison-Wesley, Boston, MA, 1982.

[11] N. Heintze and J. G. Riecke. The SLam calculus: Programming with security and integrity. In *Proc. 25th ACM Symposium on Principles of Programming Languages*, pages 365–377, San Diego, CA, Jan. 1998.

[12] K. Honda and N. Yoshida. A uniform type structure for secure information flow. In *Proc. 29th ACM Symposium on Principles of Programming Languages*, pages 81–92, Portland, OR, Jan. 2002.

[13] D. Kozen. Efficient code certification. Technical Report TR98-1661, Cornell University, Jan. 1998.

[14] D. Kozen. Language-based security. In *Proc. 24th International Symposium on Mathematical Foundations of Computer Science*, volume 1672 of *LNCS*, pages 284–298, Szklarska Poreba, Poland, Sept. 1999.

[15] C. League, Z. Shao, and V. Trifonov. Precision in practice: A type-preserving Java compiler. In *Proc. 12th International Conference on Compiler Construction*, volume 2622 of *LNCS*, pages 106–120, Warsaw, Poland, Apr. 2003.

[16] R. Medel, A. Compagnoni, and E. Bonelli. Non-interference for a typed assembly language. In *Proc. 2005 Workshop on Foundations of Computer Security*, Chicago, IL, June 2005.

[17] G. Morrisett, K. Crary, N. Glew, and D. Walker. Stack-based typed assembly language. *Journal of Functional Programming*, 12(1):43–88, Jan. 2002.

[18] G. Morrisett, D. Walker, K. Crary, and N. Glew. From system F to typed assembly language. *ACM Transactions on Programming Languages and Systems*, 21(3):527–568, Nov. 1999.

[19] A. C. Myers. JFlow: Practical mostly-static information flow control. In *Proc. 26th ACM Symposium on Principles of Programming Languages*, pages 228–241, San Antonio, TX, 1999.

[20] G. C. Necula. *Compiling with Proofs*. PhD thesis, Carnegie Mellon University, Pittsburgh, PA, Sept. 1998.

[21] G. C. Necula and P. Lee. The design and implementation of a certifying compiler. In *Proc. 98 ACM Conference on Programming Language Design and Implementation*, pages 333–344, Montreal, Canada, June 1998.

[22] F. Pottier and V. Simonet. Information flow inference for ML. *ACM Transactions on Programming Languages and Systems*, 25(1):117–158, Jan. 2003.

[23] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5–19, Jan. 2003.

[24] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proc. of the IEEE*, 63(9), Sept. 1975.

[25] F. B. Schneider, G. Morrisett, and R. Harper. A language-based approach to security. In *Informatics: 10 Years Back, 10 Years Ahead*, volume 2000 of *LNCS*, pages 86–101, 2001.

[26] F. Smith, D. Walker, and G. Morrisett. Alias types. In *Proc. 9th European Symposium on Programming*, volume 1782 of *LNCS*, pages 366–381, Berlin, Germany, Apr. 2000.

[27] G. Smith and D. Volpano. Secure information flow in a multi-threaded imperative language. In *Proc. 25th ACM Symposium on Principles of Programming Languages*, pages 355–364, San Diego, CA, Jan. 1998.

[28] D. Volpano and G. Smith. Eliminating covert flows with minimum typings. In *10th IEEE Computer Security Foundations Workshop*, pages 156–169, Washington, DC, June 1997.

[29] D. Volpano and G. Smith. A type-based approach to program security. In *Proc. 7th International Joint Conference CAAP/FASE on Theory and Practice of Software Development*, LNCS, pages 607–621, Lille, France, Apr. 1997.

[30] D. Volpano and G. Smith. Probabilistic noninterference in a concurrent language. In *Proc. 11th IEEE Computer Security Foundations Workshop*, pages 34–43, Washington, DC, June 1998.

[31] D. Walker. A type system for expressive security policies. In *Proc. 27th ACM Symposium on Principles of Programming Languages*, pages 254–267, Boston, MA, Jan. 2000.

[32] H. Xi and R. Harper. A dependently typed assembly language. In *Proc. 6th ACM International Conference on Functional Programming*, pages 169–180, Florence, Italy, Sept. 2001.

[33] S. Zdancewic and A. C. Myers. Secure information flow via linear continuations. *Higher-Order and Symbolic Computation*, 15(2–3):209–234, Sept. 2002.

A. Noninterference Proof of TAL$_C$

Lemma 3 (High Step) If $P = (H, R, I)_\kappa$, $SL(\kappa) \not\sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, then either: (1) there exists Γ_1 and $P_1 = (H_1, R_1, I_1)_\kappa$ such that $P \longmapsto P_1$, $\Psi; \Gamma_1 \vdash P_1$, $\Gamma \succeq_\theta \Gamma_1$, and $\Psi; \Gamma_1 \vdash P \approx_\theta P_1$, or (2) I is of the form ($\texttt{raise}\ \kappa'; I'$) or ($\texttt{lower}\ w$).

Proof sketch: By case analysis on the first instruction of I. I cannot be `halt`, because the typing rule for `halt` requires the context to be $\bullet$. If I is not `halt`, `raise` or `lower`, by the operational semantics and inversion on the typing rules, one can get Γ_1 and P_1 for the next step. The typing rules prohibit writing into a low heap cell, hence low heap cells remain the same after the step. When a register or stack slot is updated, Γ_1 gives it a type whose security label takes $SL(\kappa)$ into account, hence that register or stack slot has a high type in Γ_1. As a result, $\Gamma \succeq_\theta \Gamma_1$ and $\Psi; \Gamma_1 \vdash P \approx_\theta P_1$. □

Lemma 4 (Context Discharge) If $P = (H, R, I)_{\theta \triangleright w}$, $\theta \not\sqsubseteq \theta'$, $\Psi; \Gamma \vdash P$, $P \longmapsto^* (H_0, R_0, \texttt{halt}\ [\sigma])_\bullet$, then there exists Γ' and $P' = (H', R', \texttt{lower}\ w)_{\theta \triangleright w}$, such that $\Psi; \Gamma' \vdash P'$, $P \longmapsto^* P'$, $\Gamma \succeq_{\theta'} \Gamma'$, and $\Psi; \Gamma' \vdash P \approx_{\theta'} P'$.

Proof sketch: By generalized induction on the number of steps of the derivation $P \longmapsto^* (H_0, R_0, \texttt{halt}\ [\sigma])_\bullet$.

The base case of zero step is not possible, because the security contexts do not match. In the inductive case, suppose the execution consists of n steps and the proposition holds for any step number less than n. There are two cases to consider, following Lemma 3.

In the case where the first instruction of I is not `raise` or `lower`, by Lemma 3, there exists Γ_1 and P_1 such that $P \longmapsto P_1$, $\Psi; \Gamma_1 \vdash P_1$, $\Gamma \succeq_{\theta'} \Gamma_1$, $\Psi; \Gamma_1 \vdash P \approx_{\theta'} P_1$, and the security context of P_1 is the same as that of P. P_1 must be a step in between P and $(H_0, R_0, \texttt{halt}\ [\sigma])_\bullet$ because the operational semantics is deterministic. Hence by induction hypothesis on P_1, there exists Γ' and P' such that $\Psi; \Gamma' \vdash P'$, $P_1 \longmapsto^* P'$, $\Gamma_1 \succeq_{\theta'} \Gamma'$ and $\Psi; \Gamma' \vdash P_1 \approx_{\theta'} P'$. Putting the above together, $P \longmapsto^* P'$, $\Gamma \succeq_{\theta'} \Gamma'$ because $\succeq_{\theta'}$ is transitive by definition, and $\Psi; \Gamma' \vdash P \approx_{\theta'} P'$ by definition and the fact that $\Gamma_1 \succeq_{\theta'} \Gamma'$.

Case $I = \texttt{raise}\ \theta_1 \triangleright w_1; I_1$. By definition of the operational semantics, $P \longmapsto P_1$ where $P_1 = (H, R, I_1)_{\theta_1 \triangleright w_1}$. By inversion on $\Psi; \Gamma \vdash P$ and the typing rule of `raise`, $\theta \sqsubseteq \theta_1$ and $\Psi; \Gamma; \theta_1 \triangleright w_1 \vdash I_1$. By definition of well-typed programs, $\Psi; \Gamma \vdash P_1$. By induction hypothesis on P_1, there exists Γ_2 and $P_2 = (H_2, R_2, \texttt{lower}\ w_1)_{\theta_1 \triangleright w_1}$ such that $\Psi; \Gamma_2 \vdash P_2$, $P_1 \longmapsto^* P_2$, $\Gamma \succeq_{\theta'} \Gamma_2$, $\Psi; \Gamma_2 \vdash P_1 \approx_{\theta'} P_2$. $\Psi; \Gamma_2 \vdash P \approx_{\theta'} P_2$ then follows because the heaps and register files in P and P_1 are the same.

Further by the operational semantics, $P_2 \longmapsto P_3$ where $P_3 = (H_2, R_2, I_3)_\kappa$ and I_3 is the instantiated code of w_1 whose security context is κ. By inversion on the well-typedness of I (*i.e.,* $\texttt{raise}\ \theta_1 \triangleright w_1; I_1$), $\kappa = \theta \triangleright w$. By induction hypothesis on P_3, there exists Γ' and $P' = (H', R', \texttt{lower}\ w)_{\theta \triangleright w}$ such that $\Psi; \Gamma' \vdash P'$, $P_3 \longmapsto^* P'$, $\Gamma_2 \succeq_{\theta'} \Gamma'$, and $\Psi; \Gamma' \vdash P_3 \approx_{\theta'} P'$. Putting the above together, the original proposition holds for case $I = \texttt{raise}\ \theta_1 \triangleright w_1; I_1$.

Case $I = \texttt{lower}\ w_1$. By inversion on the typing rule of `lower`, $w = w_1$. Let $P' = P$, the proposition holds. □

Lemma 5 (Low Step) If $P = (H, R, I)_\kappa$, $SL(\kappa) \sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, $\Psi; \Gamma \vdash Q$, $\Psi; \Gamma \vdash P \approx_\theta Q$, $P \longmapsto P_1$, $Q \longmapsto Q_1$, then exists Γ_1 such that $\Psi; \Gamma_1 \vdash P_1$, $\Psi; \Gamma_1 \vdash Q_1$ and $\Psi; \Gamma_1 \vdash P_1 \approx_\theta Q_1$.

Proof sketch: By case analysis on the first instruction of I. By $SL(\kappa) \sqsubseteq \theta$ and the definition of $\approx_\theta$, P and Q contain the same instruction sequence. The case of raising does not change the state, hence trivially maintains the equivalence. All other cases maintain that the security context is lower than θ. Inspection on the typing rules shows that low locations in the heap can only be assigned low values. Once a register or stack slot is given a high value, its type in Γ_1 will change to high. In the case of branching, the guard must be low, so both P and Q branch to the same code. Hence the two programs remain equivalent after one step. □

Theorem 1 (Noninterference) If $P = (H, R, I)_\kappa$, $SL(\kappa) \sqsubseteq \theta$, $\Psi; \Gamma \vdash P$, $\Psi; \Gamma \vdash Q$, $\Psi; \Gamma \vdash P \approx_\theta Q$, $P \longmapsto^* (H_p, R_p, \texttt{halt}\ [\sigma_p])_\bullet$, and $Q \longmapsto^* (H_q, R_q, \texttt{halt}\ [\sigma_q])_\bullet$, then exists Γ' such that $\Psi; \Gamma' \vdash (H_p, R_p, \texttt{halt}\ [\sigma_p])_\bullet \approx_\theta (H_q, R_q, \texttt{halt}\ [\sigma_q])_\bullet$.

Proof sketch: By generalized induction on the number of steps of the derivation $P \longmapsto^* (H_p, R_p, \texttt{halt}\ [\sigma_p])_\bullet$. The base case of zero step is trivial. The inductive case is done by case analysis on the first instruction of I.

Consider the case where $I = \texttt{raise}\ \theta_1 \triangleright w_1; I_1$ and $\theta_1 \not\sqsubseteq \theta$. By definition of the operational semantics and the typing rules, $P \longmapsto P_1$ where $P_1 = (H, R, I_1)_{\theta_1 \triangleright w_1}$ and $\Psi; \Gamma \vdash P_1$. By Lemma 4, there exists Γ_2 and $P_2 = (H_2, R_2, \texttt{lower}\ w_1)_{\theta_1 \triangleright w_1}$ such that $\Psi; \Gamma_2 \vdash P_2$, $P_1 \longmapsto^* P_2$, $\Gamma \succeq_\theta \Gamma_2$, and $\Psi; \Gamma_2 \vdash P_1 \approx_\theta P_2$. Hence $\Psi \vdash H \approx_\theta H_2$ and $\Gamma_2 \vdash R \approx_\theta R_2$.

By the operational semantics, $P_2 \longmapsto P_3$ where $w_1 = l_1[\vec{\psi}]$, $P_3 = (H_2, R_2, I_3[\vec{\psi}/\Delta])_{\kappa_3}$, and $H(l_1) = \texttt{code}[\Delta]\langle\kappa_3\rangle\Gamma_3.I_3$. By inversion on the derivation of $\Psi; \Gamma_2 \vdash P_2$, $\Gamma_3 \sqsubseteq \Gamma_2$ and $\Psi; \Gamma_3 \vdash P_3$. It follows that $\Gamma_3 \vdash R \approx_\theta R_2$. By inversion on the derivation of $\Psi; \Gamma \vdash P$ where the instruction sequence of P is $\texttt{raise}\ \theta_1 \triangleright w_1; I_1$, $\kappa_3 = \kappa$.

By similarly reasoning, $Q \longmapsto^* Q_3$ where $Q_3 = (H_2', R_2', I_3)_{\kappa_3}$, $\Psi \vdash H \approx_\theta H_2'$, $\Gamma_3 \vdash R \approx_\theta R_2'$ and $\Psi; \Gamma_3 \vdash Q_3$. By transitivity of the equivalence relations, $\Psi \vdash H_2 \approx_\theta H_2'$ and $\Gamma_3 \vdash R_2 \approx_\theta R_2'$. Hence $\Psi; \Gamma \vdash P_3 \approx_\theta Q_3$. The case then follows by induction hypothesis.

All other cases remain low after a step. By Lemma 5, the two programs in the next step are equivalent and well-typed. The proof then follows by induction hypothesis. □

B. Example

Figure 15 gives a simple example to demonstrate the use of security labels and contexts. The high-level pseudo-code program involves a low variable `a` and two high variables `b` and `c`. In a corresponding TAL$_C$ program, we use heap cells labeled l_a, l_b and l_c to represent these variables. The TAL$_C$ program starts from the code labeled l_0 in a low security context. After the initial setup, it raises the security context to $\top \triangleright l_3$. The control is then transferred to the code labeled l_1, which contains a test on the high variable `b` and directs the execution to two separate branches. In either branch of the conditional, the high variable `c` is updated, and the security context is restored with `lower` l_3. The code at l_3 is then free to update the low variable `a` again.

A closer look at the code labeled l_1 reveals several interesting issues. When checking the first load instruction (`ld` $r_4, r_2(0)$), the security level for r_4 is inferred to be high ($\top$). The following branching instruction (`bnz` r_4, l_2) type-checks because the current security context ($\top \triangleright l_3$) is high enough to cover the security level of r_4. The next store instruction (`st` $r_3(0), r_0$) is also valid, because it is ok to update a high variable in a high context. In comparison, the store instruction would fail to type-check if `c` was a low variable. Finally, the high security context is ended with a lower instruction (`lower` l_3) that directs the control flow to the postdominator of the conditional.

A pseudo-code program:

```
a = 0;
if (b <> 0) then c = 1 else c = 0;
a = 1
```

A corresponding TAL$_C$ program: $(H, \{\texttt{sp} : nil\}, \texttt{jmp}\ l_0)_\bullet$ where $H = \{$

$l_a \mapsto \ \ldots$

$l_b \mapsto \ \ldots$

$l_c \mapsto \ \ldots$

$l_0 \mapsto \ \texttt{code}[\circ]\langle\bullet\rangle\{\texttt{sp} : nil\}.$
$\texttt{mov}\ r_0, 0;$ % $r_0 \leftarrow 0$
$\texttt{mov}\ r_1, l_a;$ % $r_1 \leftarrow l_a$
$\texttt{mov}\ r_2, l_b;$ % $r_2 \leftarrow l_b$
$\texttt{mov}\ r_3, l_c;$ % $r_3 \leftarrow l_c$
$\texttt{st}\ r_1(0), r_0;$ % $l_a \leftarrow 0$
$\texttt{raise}\ \top \triangleright l_3;$ % raise security context
$\texttt{jmp}\ l_1$

$l_1 \mapsto \ \texttt{code}[\circ]\langle\top \triangleright l_3\rangle\{r_0 : \langle\texttt{int}_\bot\rangle_\bot, r_1 : \langle\texttt{int}_\bot\rangle_\bot, r_2 : \langle\texttt{int}_\top\rangle_\bot, r_3 : \langle\texttt{int}_\top\rangle_\bot, \texttt{sp} : nil\}.$
$\texttt{ld}\ r_4, r_2(0);$
$\texttt{bnz}\ r_4, l_2;$ % go to l_2 if content of l_b is not zero
$\texttt{st}\ r_3(0), r_0;$ % the `else` branch: $l_c \leftarrow 0$
$\texttt{lower}\ l_3$ % restore security context and go to l_3

$l_2 \mapsto \ \texttt{code}[\circ]\langle\top \triangleright l_3\rangle\{r_0 : \langle\texttt{int}_\bot\rangle_\bot, r_1 : \langle\texttt{int}_\bot\rangle_\bot, r_2 : \langle\texttt{int}_\top\rangle_\bot, r_3 : \langle\texttt{int}_\top\rangle_\bot, \texttt{sp} : nil\}.$
$\texttt{mov}\ r_0, 1;$
$\texttt{st}\ r_3(0), r_0;$ % the `then` branch: $l_c \leftarrow 1$
$\texttt{lower}\ l_3$ % restore security context and go to l_3

$l_3 \mapsto \ \texttt{code}[\circ]\langle\bullet\rangle\{r_1 : \texttt{int}_\bot, \texttt{sp} : nil\}.$
$\texttt{mov}\ r_0, 1;$
$\texttt{st}\ r_1(0), r_0;$ % $l_a \leftarrow 1$
$\texttt{halt}\ [\texttt{int}_\bot]$

$\}$

Figure 15. TAL$_C$ example

C. Translating Linear Continuations

It may appear that TAL$_C$ is not as expressive as the language of Zdancewic and Myers' [33] (ZM), because the security context of TAL$_C$ uses static labels. Nonetheless, these static labels are only used to refer to code (e.g., that of linear continuations in ZM) whose locations can be statically determined. Indeed, their source level counterparts are the ending points of conditional structures, which are always statically known. Therefore, there is not a loss of expressiveness. We demonstrate this by speculating a translation from ZM to TAL$_C$.

In ZM, there are two expressions manipulating linear continuations: creation and elimination. The creation of a linear continuation essentially has the form $\texttt{letlin}\ y = \lambda\langle\texttt{pc}\rangle(x : \sigma).e\ \texttt{in}\ e'$. A corresponding elimination has the form $\texttt{lgoto}\ y\ v$.

The translation can be carried out following Morrisett *et al.* [18]. The step of CPS conversion is not needed because ZM is already in CPS. During closure conversion, the abstraction $\lambda\langle\texttt{pc}\rangle(x : \sigma).e$ (which corresponds to the code at a postdominator) will be assigned a static code label. This code label is exactly the static postdominator needed for raising the security context in TAL$_C$. In a formal translation, this label can be used to generate a `raise` instruction when a corresponding branching point is reached. The typing (in particular, the security labels) of a ZM program is sufficient for identifying the branching point.

The elimination of linear continuation ($\texttt{lgoto}\ y\ v$) is relatively straightforward. Suppose the code of y (the lambda abstraction) declared using `letlin` is assigned the heap label l_y during closure conversion, the elimination expression $\texttt{lgoto}\ y\ v$ can be translated as a $\texttt{lower}\ l_y$ preceded with appropriate code computing the argument v.

For better understanding the relationship between linear continuations in ZM and security contexts in TAL$_C$, we further look into an example of nested `letlin` declarations:

$$\texttt{letlin}\ y_1 = lv_1\ \texttt{in}\ \texttt{letlin}\ y_2 = lv_2\ \texttt{in}\ e.$$

Once the second `letlin` is declared, the first linear continuation y_1 should be accessible only from inside lv_2. Therefore, ZM requires that e type checks under y_2, and lv_2 type checks under y_1. This essentially enforces a stack discipline.

TAL$_C$ has a similar mechanism. Suppose the current security context is $\theta_1 \triangleright l_1$ and the current instruction sequence is $\texttt{raise}\ \theta_2 \triangleright l_2; I$. The type system of TAL$_C$ checks I under $\theta_2 \triangleright l_2$, and checks that the code type at l_2 respects $\theta_1 \triangleright l_1$. This enforces a similar stack discipline as in ZM; note that only the top stack element is apparent at any given time.

In summary, it is possible to conduct a formal translation from ZM to TAL$_C$. Nonetheless, we believe that the simple security-type system in Figure 1 of Section 2.2 is more accessible and better facilitates understanding. We leave a formal translation from ZM to TAL$_C$ as future work.