A Type System for Expressive Security Policies[*]

David Walker
Cornell University

Abstract

Certified code is a general mechanism for enforcing security properties. In this paradigm, untrusted mobile code carries annotations that allow a host to verify its trustworthiness. Before running the agent, the host checks the annotations and proves that they imply the host's security policy. Despite the flexibility of this scheme, so far, compilers that generate certified code have focused on simple type safety properties rather than more general security properties.

Security automata can specify an expressive collection of security policies including access control and resource bounds. In this paper, we describe how to instrument well-typed programs with security checks and typing annotations. The resulting programs obey the policies specified by security automata and can be mechanically checked for safety. This work provides a foundation for the process of automatically generating certified code for expressive security policies.

1 Introduction

Strong type systems such as those of Java or ML provide provable guarantees about the run-time behaviour of programs. If we type check programs before executing them, we know they "won't go wrong." Usually, the notion "won't go wrong" implies *memory safety* (programs only access memory that has been allocated for them), *control flow safety* (programs only jump to and execute valid code), and *abstraction preservation* (programs use abstract data types only as their interfaces allow). These properties are essential building blocks for any secure system such as a web browser, extensible operating system, or server that may download, check and execute untrusted programs. However, standard type safety properties alone do not enforce access control policies or restrict the dissemination of secret information.

Certified code is a general framework for verifying security properties in untrusted code. To use this security architecture, programmers and compilers must attach a collection of annotations to the code they produce. These annotations can be proofs, types, or annotations from some other kind of formal system. Regardless, there must be some way of reconstructing a proof that the code obeys a certain security policy, for upon receiving annotated code, an untrusting web browser or operating system will use a mechanical checker to verify that the program is safe before executing it. For example, Necula and Lee's proof-carrying code (PCC) implementation [20, 19] uses a first-order logic and they have shown that they can check many interesting properties of *hand-coded* assembly language programs including access control and resource bound policies [22].

In order to make certified code a practical technology, it must be possible to generate code and certificate automatically. However, so far, the compilers that emit certified code have focused on a limited set of properties. For example, the main focus of Necula and Lee's proof-generating compiler Touchstone [21] is the generation of efficient code; the security policy it enforces is the standard type and memory safety. Other frameworks for producing certified code, including Kozen's efficient code certification (ECC) [8] and Morrisett *et al.*'s [18, 16] Typed Assembly Language (TAL), concentrate exclusively on standard type safety properties.

The main reason that certified code has been used in this restricted fashion is that automated theorem provers are not powerful enough to infer properties of arbitrary programs and constructing proofs by hand is prohibitively expensive. Unable to prove security properties statically, real world security systems such as the Java Virtual Machine [12] (JVM) have fallen back on run-time checking. Run-time security checks are scattered throughout the Java libraries and are intended to ensure that applets do not access protected resources inappropriately. However, this situation is unsatisfying for a number of reasons:

- The security checks and therefore the security policy is distributed throughout library code instead of being specified declaratively in a centralized location. This can make the policy difficult to understand or change.
- There is no way to verify that checks have not been forgotten or misplaced.
- There is no way to optimize away redundant checks and certify that the resulting code is safe.

Figure 1 presents a practical alternative for producing certified code. First, we give a formal specification of a secu-

[*]This material is based on work supported in part by the AFOSR grant F49620-97-1-0013 and in part by the National Science Foundation under Grant No. EIA 97-03470. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not reflect the views of these agencies.

rity policy. When we compile a program, we use the security policy to dictate when we need to insert run-time checks to make the program secure. For example, the security policy might state that programs cannot use the network after they have read any local files. In this case, the compiler places run-time checks around every call to a network operation to ensure the program does not use the network after reading a file. Next, we optimize the program, removing run-time checks whereever we can deduce that it is safe to do so. However, when we remove a check from the program, we must leave behind enough information to be able to verify that calling the function is still safe.

When compilation has been completed, we will verify that the resulting code is safe and then link together the application program with the rest of the system. In order to ensure the security policy is obeyed, we will obviously have to use the formal policy specification. We can either do this directly or, as shown in Figure 1, we can use the specification to annotate the system interface and then compile the interface and annotations into the low-level language. For example, if the high-level system inteface contains a network API and we would like to enforce the security policy described above, we might annotate all the network functions with a pre-condition requiring that we have not yet read a file. We could then associate this pre-condition with the code that results from compiling the high-level system interface into low-level code.

This framework has a number of advantages over other security architectures. First, by defining the security policy independently of the rest of the system, it may be simpler for the implementer of the security system to write or change the policy, and easier for the applications programmers to understand it. The fact that the security policy can be defined in terms of a high-level system interface rather than its low-level implementation will also make the policy easier to understand.

Second, for a large class of security properties, we can use run-time checks to ensure that any program can be *automatically* rewritten so that it is provably secure. This mechanism relieves the programmer of the burden of constructing proofs that his or her programs obey the security policy. In fact, although programmers need to be aware of and to follow the security policy (otherwise their programs will be terminated), the programming model need not change at all.

Third, there is clear separation between the trusted and untrusted components of the system. More precisely, we must trust that:

- The formal security policy specification implies the desired semantic properties.
- The low-level system interface is correct and the code that performs run-time checks is correct.
- The verification software is correct.

However, because verification is independent of the instrumentation algorithm, we do not have to trust the application program or its compiler. Untrusted parties can write their own application-specific instrumentation and optimization transformations. In fact, programmers do not even have to use the same source language. They can write programs in different languages and then compile them into a common intermediate form or even write low-level code by hand, if they choose. Regardless of the source of the application code, it can be verified when it is linked into the extensible system.

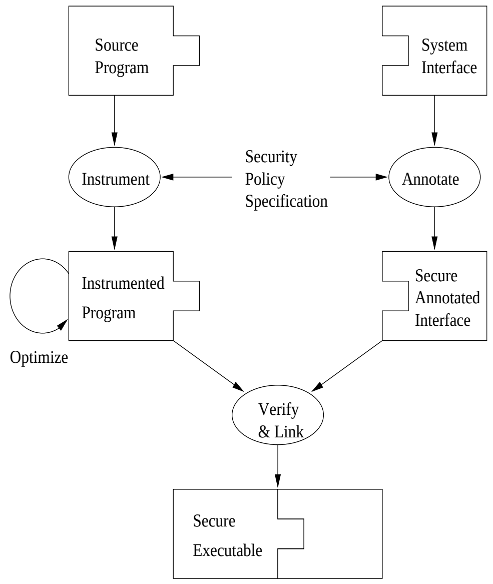

Figure 1: Architecture of a Certifying Compiler

2 Overview

In this paper, we explore one particular instance of the general framework:

- Our source language is *type-safe*. Type safety enforces many essential safety properties statically without having to resort to run-time checking. Moreover, the literature on type-directed compilation outlines many techniques for preserving typing invariants from high-level languages all the way through compilation, down to level of machine language. We will use type safety to ensure that malicious programs cannot circumvent run-time checks that will be inserted into the program to enforce more sophisticated security policies.
- Our formal security policies are specified using *security automata* [24, 27]. We have chosen security automata because they are very expressive, able to encode any *safety property* [24]. Moreover, security automaton specifications can always be enforced by inserting run-time checks. Using this mechanism, we can guarantee that we can automatically rewrite any source language program so that it is provably secure.
- Our target language is dependently-typed. In this architecture, we encode the security automaton definition in the types of the security-sensitive operations. Type-checking is sufficient to enforce the security policy. The type system that we will define is powerful enough to enforce any security automaton specification and yet is flexible enough to allow a number of optimizations.

Why use a type system? There are other frameworks for static verification. For example, Necula and Lee use a verification-condition generator that emits proof obligations in the form of first-order logic formulae with some extensions. Such a framework has clear advantages: First-order logic is extremely expressive and yet has simple proof rules. One advantage of type theory is that it handles higher-order features such as first-class functions and continuations naturally. This fact is particularly important when handling low-level languages because even the results of compiling procedural languages without function pointers are naturally higher-order: When a piece of machine code "calls" or jumps to a procedure, it passes the return address explicitly to the code it jumps to and therefore every machine-language code fragment can be thought of as a higher-order function. Our experience with low-level type systems also reveals that higher-order type constructors are extremely useful. In low-level languages, it is necessary to represent many more well-formedness invariants explicitly in the type or proof system; higher-order type constructors can help compress redundant information and are used extensively in TAL to speed type checking [15].

In practice, there are ways to work around some of these difficulties and stay within a simpler first-order system. For example, Necula and Lee fix the calling convention in their PCC implementation so they do not have to treat return addresses as first-class functions. However, this decision prevents them from performing some optimizations such as tail-call elimination. In order to keep proof-sizes small, Necula and Lee have extended conventional first-order logic with high-level language-specific axioms. Of course, each new axiom that is added should be proven consistent with the other axioms in the system, a difficult task.

Perhaps the most compelling reason for using a type system is to be able to draw upon the vast literature on type-directed compilation. Researchers already know how to preserve many kinds of typing invariants from top to bottom, through the compilation of (higher-order) modules [5, 10], closure conversion [13] and code generation [18]. It is less clear how to preserve proofs represented in other formalisms through these transformations. Therefore, by encoding security in a type system, we can immediately take advantage of existing implementation techniques and theoretical results. These well-understood techniques are what has lead researchers to focus on certifying compilers for type-safety properties in the first place. Of course, using a type system throughout compilation does not prevent implementers from encoding the final low-level results in another logic or logical framework, if they choose to do so.

The remaining sections of this paper describe our approach to security in more detail. First, in Section 3, we present security automata, our mechanism for specifying security policies. Our presentation is derived from work by Úlfar Erlingsson and Fred Schneider [24, 27]. Next, in Section 4, we define a generic typed target language, $\lambda_{\mathcal{A}}$, for our compiler. This language is a dependently-typed lambda calculus that can encode any security automaton specification. The formulation of the language is the main technical contribution of the paper: It is flexible enough to allow a number of interesting optimizations and yet prevents malicious programs from circumventing security checks. After defining the generic language, we explain how to automatically construct a typed interface that will specialize the language so that it enforces the policy of a particular automaton. Finally, in Section 5, we show how to automatically instrument programs written in a high-level language (the simply-typed lambda calculus) and discuss possible optimizations to the procedure. The last section discusses additional related work.

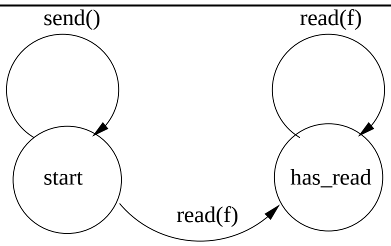

Figure 2: Security Automaton for a File System Policy

3 Security Automata

Security policies will be specified independently of any particular programming language using *security automata* [24]. These automata are defined similarly to other automata [7]: They possess a set of states and rules for making transitions from one state to the next. The author of the security policy determines the set of states and the transition relation. One of these states is designated as the *bad* state and entry into this state is defined to be a violation of the security policy.

Security automata enforce safety properties by monitoring programs as they execute. Before an untrusted program is allowed to execute a security-sensitive or *protected* operation, the security automaton checks to see if the operation will cause a transition to the *bad* state. If so, the automaton terminates the program. If not, the program is allowed to execute the operation and the security automaton makes a transition to a new state. For example, a web browser might allow applets to open and read files, and send bits on the network. However, assuming the web browser wants to ensure some level of privacy, the open, read, and send operations will be designated protected operations. Before an untrusted applet can execute one of these functions, the browser will check the security automaton definition to ensure the operation is allowed in the current state.

By monitoring programs in this way, security automata are sufficiently powerful that they can restrict access to private files or bound the use of resources. They can also enforce the safety properties typically implied by type systems such as memory safety and control-flow safety. In fact, security automata can enforce any *safety property* [24]. However, some interesting security policies including information flow, resource availability, and general liveness properties are not safety properties and cannot be enforced by this mechanism. Nevertheless, Schneider [24] points out that some of these applications can still use a security automaton: The automaton must simply enforce a stronger property than is required. For example, the policy that admits any program that allocates a finite amount of memory cannot be enforced by a security automaton. However, security automata can enforce the policy that prevents a program from allocating more than an *a priori* fixed amount (such as 1 MB) of memory. The latter policy reduces the number of legal programs that can be written (a program that allocates 1.1 MB will be prematurely terminated), but it may be effective in practice.

Figure 2 depicts a security automaton that enforces the simple policy that programs must not perform a send on the network after reading a file. The security automaton actually has three states: the *start* state, the *has_read* state, and the *bad* state, which is not shown in the diagram. For the purpose of this example, there are only two protected operations: the *send* operation and the *read* operation. Each of the arcs in the graph is labeled with one of these operations

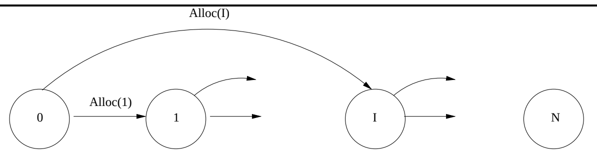

Figure 3: Security Automaton for a Memory Bounds Policy

Q	a finite or countably infinite set of states
q_0	a distinguished initial state
bad	the single "bad" state
F	a finite set of function symbols (f)
A	a countable set of constants (a)
δ	a computable (deterministic) total function: $\mathrm{F} \to (Q \times \vec{\mathrm{A}}) \to Q$

Figure 4: Elements of a Security Automaton

and indicates the state transition that occurs when the operation is invoked. If there is no outgoing arc from a certain state labeled with the appropriate operation, the automaton makes a transition to the *bad* state. For example, there is no *send* arc emanating from the *has_read* state. Consequently, if a program tries to use the network in the *has_read* state, it will be terminated.

Figure 3 shows a second security automaton that restricts the amount of heap memory that a program can allocate. The states are indexed by the natural numbers 0 through N and the protected operation $alloc(I)$ causes an automaton transition from state S to state $S + I$, provided $S + I$ is less than or equal to N.

3.1 Formal Definitions

For our purposes, a security automaton ($\mathcal{A}$) is a 6-tuple containing the fields summarized in Figure 4. Like other automata, a security automaton has a set of states Q (either finite or a countably infinite), and a distinguished initial state q_0. The automaton also has a single bad state (bad). Entrance into the bad state indicates that the security policy has been violated. All other states are considered "good" or "accepting" states. The automaton's inputs correspond to the application of a function symbol f to arguments $a_1, \ldots, a_n$ where f is taken from the set F (the set of protected operations) and $a_1, \ldots, a_n$ are taken from A.

A security automaton defines allowable behaviour by specifying a transition function δ. Formally, δ is a deterministic, total function with a signature $\mathrm{F} \to (Q \times \vec{\mathrm{A}}) \to Q$ where $\vec{\mathrm{A}}$ denotes the set of lists $a_1, \ldots, a_n$. Upon receiving an input $f(a_1, \ldots, a_n)$, an automaton makes a transition from its current state to the next state as dictated by this transition function. If the security policy permits the operation f on arguments $a_1, \ldots, a_n$ in the current state q then the next state, $\delta(f)(q, a_1, \ldots, a_n)$, will be one of the "good" ones. On the other hand, if the security policy disallows the operation then $\delta(f)(q, a_1, \ldots, a_n)$ will equal bad. Furthermore, once the automaton enters the bad state, it stays there. Formally, for all f and $a_1, \ldots, a_n$, $\delta(f)(bad, a_1, \ldots, a_n) = bad$.

The transition function δ must also be computable. Moreover, the implementor of the security policy must supply code for a family of functions δ_f such that $\delta_f(q_1, a_1, \ldots, a_n)$ equals $\delta(f)(q_1, a_1, \ldots, a_n)$. In the following sections, we will use these functions to instrument untrusted code with security checks.

The language accepted by the automaton $\mathcal{A}$, written $\mathcal{L}(\mathcal{A})$, is a set of strings where a string is a finite sequence of symbols $s_1, \ldots, s_n$ and each symbol s_i is of the form $f(a_1, \ldots, a_m)$. The string $s_1, \ldots, s_n$ belongs to $\mathcal{L}(\mathcal{A})$ if the predicate $Accept(q_0, s_1, \ldots, s_n)$ holds where $Accept$ is the least predicate such that:

Definition 1 (String Acceptance) *For all states q and (possibly empty) sequences of symbols $s_1, \ldots, s_n$, $Accept(q, s_1, \ldots, s_n)$ if $q \neq bad$ and:*

1. *$s_1, \ldots, s_n$ is the empty sequence or*
2. *$s_1 = f(a_1, \ldots, a_m)$ and $\delta(f)(q, a_1, \ldots, a_m) = q'$ and $Accept(q', s_2, \ldots, s_n)$*

3.2 The File System Policy

We can now define the file system policy described in the previous section. Infomally, the policy states that no network send is allowed after any file is read. For the sake of future examples, we extend this policy slightly by restricting access to some files; in order to determine whether or not the applet has access to the file a, we will have to invoke the function $read?(a)$, which has been provided by the implementor of the file system.

The corresponding security automaton has three states: *start*, the initial state; *has_read*, the state we enter after any file read; and, of course, the *bad* state. The protected operations, F, are *send* and *read* and the constants, A, include all files and the integers. The transition function δ, written in pseudo-code, is the following:

```
$\delta_{send}(q)$ =
    if $q = start$ then
        $start$
    else
        $bad$

$\delta_{read}(q, a)$ =
    if $q = start \wedge read?(a)$ then
        $has\_read$
    else if $q = has\_read \wedge read?(a)$ then
        $has\_read$
    else
        $bad$
```

3.3 Enforcing Security Automaton Policies

We can enforce the policies specified by security automata by instrumenting programs with run-time security checks. For example, according to the file system policy from the previous section, we must be in the *start* state in order for the *send* to be safe. A program instrumentation tool could enforce this policy by wrapping the code invoking *send* with security checks:

```
let next = δ_send(current) in
if next = bad then halt
else send()
```

The first statement invokes the security automaton to determine the next state given that a *send* operation is invoked in the current state. The second statement tests the next state to make sure it is not the *bad* one. If it is *bad*, then program execution is terminated using the halt instruction.

After performing the initial transformation that wraps all protected operations with run-time security checks, a program optimizer might attempt to eliminate redundant checks by performing standard program optimizations such as loop-invariant removal and common subexpression elimination. An optimizer might also use its knowledge of the special structure of a security automaton to eliminate more checks than would otherwise be possible.

An implementation developed by Erlingsson and Schneider [27] attests to the fact that security automata can enforce a broad, practical set of security policies. Their tool, SASI, automatically instruments untrusted code with checks dictated by a security automaton specification and optimizes the output code to eliminate checks that can be proven unnecessary. SASI is both flexible and efficient and they have implemented a variety of security policies from the literature. For example, using SASI for the Intel Pentium architecture, they have specified the memory and control-flow safety policy enforced by Software Fault Isolation (SFI) [28]. The SASI-instrumented code is only slightly slower than the code produced by the special-purpose, hand-coded MiSFIT tool for SFI [25]. As another example, using SASI for the Java Virtual Machine, they have been able to reimplement the security manager for Sun's Java 1.1. The SASI-instrumented code is equally as efficient as the Java security manager in some cases and more efficient in others. Because the SASI security policy is specified separately from the rest of the Java system, it is simpler to modify than in the current system.

4 A Secure Typed Target Language

Previous implementations of security automaton enforcement mechanisms could enforce mobile code security by downloading applet source code, instrumenting the code with security checks and then optimizing away redundant run-time checks. As discussed in the introduction, these schemes suffer from the fact that the entire compiler and optimizer, complicated pieces of code, become part of the trusted computing base. Moreover, unless some form of cryptography is used, compilation must be performed on-line at the host site.

In this section, we explain the design of a dependently-typed target language that is powerful enough to encode policies described by security automata. Because the type system alone is sufficient to enforce the security policy, the compiler and optimizer are not part of the trusted computing base. Moreover, provided the security policy is published, unknown and untrusted principals can compile and optimize their programs off-line. The host computer can later download the resulting low-level programs and check them for safety automatically.

The type system that we will present is relatively complicated, so a reasonable question to ask is how much this complexity will impact the trusted computing base. Fortunately, little of the type system is specialized to encode security automata in particular. For example, the basic building blocks of the language are polymorphism, singleton types, and existential types. Strongly-typed languages for optimizing data representations like TAL or Dependent ML [33] already contain these type constructors so that they can safely solve other data representation problems. For example, singleton types are useful for representing arrays and performing array bounds check elimination [32] as well as representing tagged unions. The TIL(T) and FLINT compilers use existential types to encode closures [13] and Java classes [9], respectively. Polymorphism is ubiquitous. Therefore, there can be significant reuse of many of the type constructors in our language. This fact eases the implementation burden and makes the trusted computing base more manageable. It also reduces the proof obligations by presenting a uniform framework for reasoning about code, data, and security; later in this section, we will prove a single soundness result that implies both the normal type safety properties and that the policy specified by a security automaton is enforced.

On the other hand, in order to represent security automaton state and transition function, the typing rules for the language manipulate a state component and a collection of predicates, which are less standard features for a type system. Still, these features do appear elsewhere in type systems for low-level language. For instance, TAL contains a state component for reasoning about aliasing and stateful operations such as object deallocation [26]. Both Dependent ML and TAL contain a collection of predicates for reasoning about arithmetic so that programs can eliminate array bounds checks.

4.1 An Informal Introduction

In order to ensure protected operations are used safely, each operation is given a type that contains a collection of predicates. These predicates specify a function precondition and they must be proven before the function can be called. For example, in order to enforce our file system policy, the type of the *send* operation could include these predicates:

$$\begin{array}{l} P_1 : \delta_{send}(current, next) \\ P_2 : next \neq bad \end{array}$$

These predicates state that executing the *send* operation causes a transition from the state *current* to the state *next*, and moreover, that the *next* is not *bad* so the security policy will not be violated. Upon return, the type of the *send* operation will indicate that the automaton is in state *next*

Each time *send* or another protected function is invoked, the type checker must be able to prove that the calling context satisfies the precondition. If it can do so, the program satisfies the security policy. However, in general, given an arbitrary program, a theorem prover will not be able to prove all preconditions are satisfied in all cases. Consequently, programs will have to contain run-time security checks. These security checks will be given types that express post-conditions containing information about the automaton transition function. The post-conditions make proving the preconditions on the protected operations easy.

The following example demonstrates how we can verify that the wrapper code for the *send* operation is safe:

```
let $next$ = $\delta_{send}(current)$ in
$P_1$:  $\delta_{send}(current, next)$
if $next$ = $bad$ then $\cdots$
else
    $P_2$: $next \neq bad$
    $send()$
```

Predicate P_1 is the post-condition for the δ_{send} function and predicate P_2 can be inferred given the test in the conditional statement. The predicates P_1 and P_2, together with the information that the automaton is in the state *current*, are sufficient to prove that the precondition on the *send* operation has been satisfied.

In order to ensure the last condition is met (*i.e.* that the automaton is in the state described by the data structure *current*), the type system cannot trust the programmer to manipulate the state data structures properly. For instance, the type system must prevent a malicious programmer from substituting some unrelated state *current′* for the proper state *current* in the code above. The type system prevents such behaviour by statically keeping track of the current state itself. Below, the comments $state : X$ indicate what the type checker knows about the current state. We start out assuming the type checker knows that the state is equal to *current*. Notice that the type checker trusts that the protected function *send* has been given an accurate type and therefore after calling that function, it believes the state is *next*:

```
state : current                    (*)
let next = δ_send(current) in      (**)
state : current
if next = bad then halt            state : current
else send()                        state : next
```

So far during this informal explanation, we have been a little sloppy. On line (**) above, *current* is value variable that is used *at run-time*, but on line (*), *current* is part of a *compile-time* expression (and similarly for *current*, *next* and δ_{send} in the previous code fragment). In order to avoid passing around values that are only used to make code type check (thereby incurring unnecessary run-time costs), we need to have a clear distinction between run-time and compile-time objects. From now on, we will use hat notation to distinguish between compile-time ($\hat{x}$) and run-time objects (x) whenever there might be ambiguity.

Despite this necessary separation, we must still be able to reflect information gained by run-time tests into the static type system, as we did in the example above. Singleton types are one of the mechanisms that will help us towards this goal. For example, if a variable x has type $\mathtt{S}(\widehat{start})$, then we not only know that x represents a state, but also that x represents the particular state *start*. The singleton type reflects very precise information (information that could have been obtained via a run-time test) into the type system.

Unfortunately, when used in isolation, singleton types are actually *too precise* for most situations. In the example above, the reason that we are performing a dynamic test is because we do not know exactly which state we are in! Perhaps we have passed a join point in the code or returned from an unknown function. In these cases, it is impossible to give a value a precise type such as $\mathtt{S}(\widehat{start})$.

Our solution to this problem is standard: Add polymorphism. When we reach a join in the code, we may not know the exact state statically, but we can arrange to know that we are in some some state ϱ (where ϱ is a type variable). We can also arrange to thread a value through the computation, say *current*, that represents the unknown state. We give that value the singleton type $\mathtt{S}(\varrho)$. To recover precise information about the current state and to propagate that information into the type system, we will perform a dynamic test on *current*.

Once we have added singleton types for automaton states, it is straight-forward to add singleton types for other values as well. We will need these singletons if we would like to encode policies that depend upon values other than just the current state. For example, in our simple file system policy, the right to read a file depends upon exactly which file is requested for reading. In the memory bounds policy, the right to allocate memory depends upon exactly how much more memory has been requested.

The last type constructor we will use is the existential type. In order to allow values with singleton types to be stored in data structures, such as arrays or lists, without again making the type of the array or list too precise, we use existential types. More generally, escaping singletons with type $\mathtt{S}(P)$ can be encapsulated using an existential type $\exists\varrho{:}\mathtt{State}.\mathtt{S}(\varrho)$, and used generically. For example, the type $\exists\varrho{:}\mathtt{Val}.int(\varrho)$ can be used as an unspecific, ordinary integer throughout the "security-insensitive" code (such as the math library, for instance), but when the appropriate time comes (the code invokes a security-sensitive operation), the existential can be opened up and the necessary dependencies created. We use this property to simplify the formal instrumentation procedure.

4.2 Formal Definitions

Formally, the target language contains three main parts: the predicates P, the types τ, and the term level constructs. We will explain each of these parts in succession. Figure 5 presents the syntax of the entire language.

Predicates Predicates, P, may be variables ρ or ϱ, indices (constant predicates) ι, or functions of a number of arguments $\iota(P_1, \ldots, P_n)$. All of these predicates are compile-time only objects. Predicates are further divided into three distinct kinds:

- Predicates that correspond to values of base type.[1] For each value a of base type, there is a corresponding index $\hat{a}$ of kind $\mathtt{Val}$. By convention, we use ρ for variables of kind $\mathtt{Val}$.
- Predicates that correspond to security automaton states. For each automaton state q, there is a corresponding index $\hat{q}$ of kind $\mathtt{State}$. By convention, we use ϱ for variables of kind $\mathtt{State}$.
- Predicates that describe relations between values and/or states. These predicates have kind $(\kappa_1, \ldots, \kappa_n) \to \mathcal{B}$ where $\mathcal{B}$ is the boolean kind.

The last kind of predicate serves two purposes. Predicates of the form $\delta_{send}(P_{q_1}, P_{q_2})$ describe the automaton transition function; they may be read as "in state P_{q_1}, executing the send operation causes a transition to state P_{q_2}." A special predicate $\neq(\cdot,\cdot)$ of kind $(\mathtt{State}, \mathtt{State}) \to \mathcal{B}$ will be used to denote the fact that some state q is not equal to the *bad* state and consequently that it is safe to execute an operation that causes a transition into q.

We specify the well-formedness of predicates using the judgement $\Phi \vdash P : \kappa$ where Φ is a type-checking context containing three components: a predicate context Δ, a finite map Γ from value variables to types, and another predicate P' indicating the current state of the automaton. The latter two components are not used for specifying the well-formedness of predicates (they will be used for type-checking terms). The signature $\mathcal{I}$ assigns kinds to the indices. Kinds for variables are determined by the predicate context Δ. The kind of a function symbol must agree with the kinds of the predicates to which it is applied. Due to space considerations, the formal rules have been omitted (see the technical report [29] for details).

[1]In order to simplify the presentation, we only consider policies that depend upon values of base type here. See Section 4.5 for further explanation.

kinds	κ	$::=$	$\texttt{Val} \mid \texttt{State} \mid \mathcal{B} \mid (\kappa, \ldots, \kappa) \to \mathcal{B}$
indices	$\iota, \hat{a}, \hat{q}$		
index sig	$\mathcal{I}$	$:$	*indices* $\to$ *kinds*
pred. vars	ρ, ϱ		
predicates	P	$::=$	$\rho \mid \iota \mid \iota(P_1, \ldots, P_n)$
predicate ctxt	Δ	$::=$	$\cdot \mid \Delta, \rho{:}\kappa \mid \Delta, P$
base types	b	$\in$	$\mathrm{BaseType} + \texttt{S}$
types	τ	$::=$	$b(P) \mid \forall[\Delta].(P, \tau_1, \ldots, \tau_n) \to \texttt{0} \mid \exists\rho{:}\kappa.\tau$
constants	a, q, f		
constant sig	$\mathcal{C}$	$:$	*constants* $\to$ *types*
value vars	g, x		
values	v	$::=$	$x \mid a \mid \texttt{fix}\, g[\Delta].(P, x_1{:}\tau_1, \ldots, x_n{:}\tau_n).e \mid v[P] \mid v[\cdot] \mid \texttt{pack}[P, v]$ *as* τ
expressions	e	$::=$	$v_0(v_1, \ldots, v_n) \mid \texttt{halt} \mid \texttt{let}\, \rho, x = \texttt{unpack}\, v\, \texttt{in}\, e \mid \texttt{if}\, v\, (q \to e_1 \mid \_ \to e_2)$

Figure 5: Syntax of $\lambda_{\mathcal{A}}$

Figure 6 gives the rules for proving predicates. The judgement $\Phi \vdash P$ indicates that the boolean-valued predicate P is true, and the judgement $\Phi \vdash P$ in_state indicates that the program is currently executing in the automaton state P.

Aside from the special predicate $\neq(\cdot,\cdot)$, our predicates are completely uninterpreted. This decision makes it trivial to show the decidability of the type system. However, some optimizations may not be possible without a stronger logic. To remedy this situation, implementers may add axioms to the type system provided they also supply a decision procedure for the richer logic. In Section 5.2, we show how to add security policy-specific axioms that allow many unnecessary security checks to be eliminated.

Types As discussed in the previous section, we reflect values into the type structure using the singleton types $b(P)$ (where b is a base type and P has kind $\texttt{Val}$) and $\texttt{S}(P)$ (where P has kind $\texttt{State}$).

The second main type constructor is a polymorphic function type $\forall[\Delta].(P, \tau_1, \ldots, \tau_n) \to \texttt{0}$. The predicate context Δ abstracts a series of predicate variables and requires that a sequence of boolean-valued predicates be satisfied before the function can be invoked. The predicate P in the first argument position is not a run-time argument to the function. Rather, it is another precondition requiring that the function be called in the state associated with P. The actual function arguments must have types τ_1 through τ_n.

The notation "$\to$0" at the end of each function type is intended to indicate that functions in our language do not "return" the way high-level language functions normally do. All functions are written in continuation-passing style (CPS) so they are passed their return address (another function) explicitly and "return" by calling that function. We have chosen to present the language in CPS for two reasons. First, CPS linearizes the code and makes the flow of control evident; this is convenient for the type system because it must thread the static state component along the control-flow path. Second, CPS makes all run-time control transfers and compile-time information transfers occur using the same mechanism. In the latter case, this means that we can control how information is propagated at all join points in the code (function returns, if statements) using the same uniform mechanism: polymorphic instantiation. If we did not use CPS then we would need some special syntax to accomplish these joins on if statements and upon return from functions. Still, it may be useful in an implementation to add such special cases.

As mentioned above, the language also includes existential types of the form $\exists\rho{:}\kappa.\tau$.

We specify the well-formedness of types using the judgement $\Phi \vdash \tau$. In general, a type is well-formed if Δ contains the free variables of the type. Function types of the form $\forall[\Delta].(P, \tau_1, \ldots, \tau_n) \to \texttt{0}$ also require that P has kind $\texttt{State}$ and that the predicates occuring in Δ have kind $\mathcal{B}$. The formal rules may be found in the technical report [29]. Because predicates are uninterpreted, we can use standard syntactic equality of types up to α-conversion of bound variables.

Values and Expressions The typing rules for values have the form $\Phi \vdash v : \tau$ and state that the value v has type τ in the given context. The judgement $\Phi \vdash e$ states that the expression e is well-formed. Recall that CPS expressions do not return values, and hence the latter judgement is not annotated with a return type. Figure 6 presents the formal rules. In these judgements, we use the notation $\Phi, \rho{:}\kappa$ to denote a new context in which the binding $\rho{:}\kappa$ has been appended to the list of assumptions in Φ. The operation is undefined if ρ appears in Φ. The notations Φ, P and $\Phi, x{:}\tau$ and the extension to Φ, Δ are similar, although P may already appear in Φ.

The values include variables and constants. The treatment of variables is standard, and a signature $\mathcal{C}$ gives types to the constants.

The value $v[P]$ is the instantiation of the polymorphic value v with the predicate P. We consider this instantiation a value because predicates are used only for type-checking purposes; they have no run-time significance. The value $v[\cdot]$ is somewhat similar: If v has type $\forall[P, \Delta].(\cdots) \to \texttt{0}$ and we can prove the predicate P is valid in the current context, we give $v[\cdot]$ the type $\forall[\Delta].(\cdots) \to \texttt{0}$. Again, the notation $[\cdot]$ is used only to specify that the type-checker should attempt to prove the precondition; it will not influence the execution of programs. In a system with a more sophisticated logic than the one presented in this paper, we might not want to trust the correctness of complex decision procedures for the logic. In this case, we would replace $[\cdot]$ with a proof of the precondition and replace the type checker's decision procedure with a much simpler proof-checker.

Target language function values specify a list of preconditions using the predicate context Δ. Every function also expresses a state precondition P. The function can only

$\boxed{\Phi \vdash P \qquad \Phi \vdash P \text{ in\_state}}$

$$\frac{}{\Delta_1, P, \Delta_2; \Gamma; P' \vdash P} \tag{1}$$

$$\frac{}{\Phi \vdash \neq (\hat{q}, \hat{q}')} \; (\hat{q} \neq \hat{q}') \tag{2}$$

$$\frac{}{\Delta; \Gamma; P \vdash P \text{ in\_state}} \tag{3}$$

$\boxed{\Phi \vdash v : \tau}$

$$\frac{}{\Phi \vdash x : \tau} \; (\Phi(x) = \tau) \tag{4}$$

$$\frac{}{\Phi \vdash a : \tau} \; (\mathcal{C}(a) = \tau) \tag{5}$$

$$\frac{\begin{array}{c}\Phi \vdash \tau_g \\ (\Phi, \Delta, g{:}\tau_g, x_1{:}\tau_1, \ldots, x_n{:}\tau_n) \leftarrow P \vdash e\end{array}}{\Phi \vdash \mathtt{fix}\, g[\Delta].(P, x_1{:}\tau_1, \ldots, x_n{:}\tau_n).e : \tau_g} \tag{6}$$

(where $\tau_g = \forall[\Delta](P, \tau_1, \ldots, \tau_n) \rightarrow 0$)

$$\frac{\Phi \vdash v : \forall[\rho{:}\kappa, \Delta].(P', \tau_1, \ldots, \tau_n) \rightarrow 0 \quad \Phi \vdash P : \kappa}{\Phi \vdash v[P] : (\forall[\Delta].(P', \tau_1, \ldots, \tau_n) \rightarrow 0)[P/\rho]} \tag{7}$$

$$\frac{\Phi \vdash v : \forall[P, \Delta].(P', \tau_1, \ldots, \tau_n) \rightarrow 0 \quad \Phi \vdash P}{\Phi \vdash v[\cdot] : \forall[\Delta].(P', \tau_1, \ldots, \tau_n) \rightarrow 0} \tag{8}$$

$$\frac{\Phi \vdash P : \kappa \quad \Phi \vdash v : \tau[P/\rho]}{\Phi \vdash \mathtt{pack}[P, v] \; \mathit{as} \; \exists\rho{:}\kappa.\tau : \exists\rho{:}\kappa.\tau} \tag{9}$$

$\boxed{\Phi \vdash e}$

$$\frac{\begin{array}{c}\Phi \vdash v_0 : \forall[].(P, \tau_1, \ldots, \tau_n) \rightarrow 0 \\ \Phi \vdash v_1 : \tau_1 \quad \cdots \quad \Phi \vdash v_n : \tau_n \\ \Phi \vdash P \text{ in\_state}\end{array}}{\Phi \vdash v_0(v_1, \ldots, v_n)} \tag{10}$$

$$\frac{}{\Phi \vdash \mathtt{halt}} \tag{11}$$

$$\frac{\Phi \vdash v : \exists\rho{:}\kappa.\tau \quad \Phi, \rho{:}\kappa, x{:}\tau \vdash e}{\Phi \vdash \mathtt{let}\, \rho, x = \mathtt{unpack}\, v \,\mathtt{in}\, e} \tag{12}$$

$$\frac{\begin{array}{c}\Phi \vdash v : \mathtt{S}(\rho) \qquad \Phi \vdash q : \mathtt{S}(\hat{q}) \\ \Phi' \vdash e_1[\hat{q}/\rho] \qquad \Phi, \neq (\rho, \hat{q}) \vdash e_2\end{array}}{\Phi \vdash \mathtt{if}\, v\, (q \rightarrow e_1 \mid \_ \rightarrow e_2)} \tag{13}$$

(where $\Phi = \Delta, \rho{:}\mathtt{State}, \Delta'; \Gamma; P$
and $\Phi' = \Delta, (\Delta'[\hat{q}/\rho]); \Gamma[\hat{q}/\rho]; P[\hat{q}/\rho]$)

$$\frac{\begin{array}{c}\Phi \vdash v : \mathtt{S}(\hat{q}) \qquad \Phi \vdash q : \mathtt{S}(\hat{q}) \\ \Phi \vdash e_1\end{array}}{\Phi \vdash \mathtt{if}\, v\, (q \rightarrow e_1 \mid \_ \rightarrow e_2)} \tag{14}$$

$$\frac{\begin{array}{c}\Phi \vdash v : \mathtt{S}(P) \qquad \Phi \vdash q : \mathtt{S}(\hat{q}) \\ \Phi, \neq (P, \hat{q}) \vdash e_2\end{array}}{\Phi \vdash \mathtt{if}\, v\, (q \rightarrow e_1 \mid \_ \rightarrow e_2)} \; \begin{pmatrix} P \neq \rho \\ P \neq \hat{q} \end{pmatrix} \tag{15}$$

Figure 6: Static Semantics

be called in the state denoted by P. Static semantics rule (10) contains the the judgement $\Phi \vdash P$ in_state, which ensures this invariant is maintained. This rule also enforces the standard constraints that argument types must match the types of the formal parameters. Finally, because the predicate context is empty, any preconditions the function might have specified must have already been proven valid.

Rule (6) states that we type check the body of a function assuming its preconditions hold. In this rule, we use the notation $\Phi \leftarrow P$ to denote a context Φ' in which the state component of Φ has been replaced by P. For example, suppose a function g is defined in the context $\Delta'; \Gamma'; P'$. The type checker can use any of the predicates in Δ' to help prove g is well-formed but it cannot assume that g will be called in the state P'. The function g is defined here, but may not be used until much later in the computation when the state is different (P'' perhaps).

It is tempting to define a predicate "*in_state*(P)" and to include this predicate in the list of function preconditions Δ. Using this mechanism, it may appear as though we could eliminate the special-purpose state component of the type-checking context. Unfortunately, this simplification is unsound. Consider the following informal example:

```
% Assume current state = $start$
let $g{:}\forall[in\_state(start)].(\tau_1, \ldots, \tau_n) \rightarrow 0 = \cdots$ in
% Prove precondition:
let $g'{:}\forall[\,].(\tau_1, \ldots, \tau_n) \rightarrow 0 = g[\cdot]$ in
% Change the state to $q'$ where $q' \neq start$:
let $\_ = op()$ in
% $g$ is not called in the $start$ state!
$g'(v_1, \ldots, v_n)$
```

On the last line, the function g is invoked in a state q' when the function definition assumed it would be invoked in the *start* state. The example highlights the main difference between the state predicates and the others: The validity of the predicates in Δ is invariant throughout the execution of the program whereas the validity of a state predicate varies during execution because it depends implicitly on the current state of the machine.

Existential values are handled in standard fashion [14]. The value $\mathtt{pack}[P, v]$ *as* $\exists\rho{:}\kappa.\tau$ creates an existential package that hides P in τ using ρ. The corresponding elimination form, $\mathtt{let}\, \rho, x = \mathtt{unpack}\, v' \,\mathtt{in}\, e$ unpacks the existential v', substituting v for x and P for ρ into the remaining expression e. As with polymorphic types, we assume a type-erasure interpretation of existentials.

Finally, the conditional $\mathtt{if}\, v\, (q \rightarrow e_1 \mid \_ \rightarrow e_2)$ tests an automaton state v to determine whether v is the state q or not. If so, the program executes e_1 (see rule (13)) and if not, the program executes e_2. A variant of Harper and Morrisett's typecase [6] operator, `if` also performs type refinement. If v has type $\mathtt{S}(\rho)$ then it refines the type-checking context with the information that $\rho = \hat{q}$ by substituting $\hat{q}$ for ρ. On the other hand, if v is not q, the second branch is taken and the context is refined with the information $\neq (\rho, \hat{q})$. Programs can use this mechanism to dynamically check whether or not they are about to enter the bad state and prevent it.

There is no need to use the $\mathtt{if}\, v$ construct if we know which state a value v represents. For example, we know the expression $\mathtt{if}\, q\, (q \rightarrow e_1 \mid \_ \rightarrow e_2)$ will reduce to e_1 and therefore e_2 is dead code and the test is wasted computation. However, during the proof of soundness of the type system, such configurations arise and cause difficulties. To avoid these difficulties, we follow the strategy of Crary *et al.* [1] and add the *trivialization* rules (14) and (15) which deal

$$v(v_1,\ldots,v_n) \longmapsto_{\cdot} e_m[v, v_1,\ldots,v_n/g, x_1,\ldots,x_n] \qquad \begin{array}{l} \text{if } v = v'\,\phi_1\cdots\phi_m \\ \text{and } v' = \mathtt{fix}\,g[\theta_1,\ldots,\theta_m].(x_1{:}\tau_1,\ldots,x_n{:}\tau_n).e_0 \\ \text{and for } 1\le i\le m, \\ \quad \phi_i=[\cdot] \text{ and } \theta_i=P_i \text{ and } e_i=e_{i-1}, \text{ or} \\ \quad \phi_i=[P_i'] \text{ and } \theta_i=\rho_i{:}\kappa_i \text{ and } e_i=e_{i-1}[P_i'/\rho_i] \end{array}$$

$$\mathtt{let}\,\rho,x=\mathtt{unpack}\,(\mathtt{pack}[P,v]\ \mathit{as}\ \tau)\,\mathtt{in}\,e \longmapsto_{\cdot} e[P,v/\rho,x]$$

$$\mathtt{if}\,q'\,(q\to e_1 \mid \_\to e_2) \longmapsto_{\cdot} e_1 \qquad \text{if } q'=q$$

$$\mathtt{if}\,q'\,(q\to e_1 \mid \_\to e_2) \longmapsto_{\cdot} e_2 \qquad \text{if } q'\neq q$$

Figure 7: Operational Semantics for $\lambda_{\mathcal{A}}$

with these redundant cases. Each rule type checks only the branch of the if statement that will be taken.

Operational Semantics The operational semantics for the language is given by the relation $e \longmapsto_s e'$ (see Figure 7). The symbol s is either empty $(\cdot)$ or it is a protected function symbol applied to some number of arguments $(f(a_1,\ldots,a_n))$. Most operations, and, in fact, all of the operations shown in Figure 7, emit the empty symbol. However, this figure does not show the operation of the protected functions. In the next section, we will explain the operational semantics of the protected functions f in the context of a signature for a particular security automaton.

We have given a typed operational semantics to facilitate the proof of soundness of the system. However, inspection of the rules will reveal that evaluation does not depend upon types or predicates, provided the expressions are well-formed. Therefore we can type-check a program and then erase the types before executing it.

4.3 The Secure System Interface

In order to specialize the generic language, we construct a typed interface or *signature* for the constants in the language. This is the system interface that untrusted code will link against. Recall from the introduction that application programmers follow their regular routine of programmming in a high-level language against a high-level system interface. We need to obtain the secure target language interface from this high-level interface and the security automaton definition.

We assume that the high-level interface for constants a and protected operations f is given by a signature $\mathcal{C}_{source}$ where $\mathcal{C}_{source}(a)$ is some base type b and $\mathcal{C}_{source}(f)$ is some function type taking a single continuation $(b_1,\ldots,b_n,(b)\to 0)\to 0$. Now, we can choose a security automaton $\mathcal{A}$ to define which operations $f(a_1,\ldots,a_n)$ are allowed (the continuation does not influence this decision). Together then, the automaton $\mathcal{A}$ and signature $\mathcal{C}_{source}$ are use to define the target language interface. This definition is presented in Figure 8 and has three parts: the type signature $\mathcal{I}$, the value signature $\mathcal{C}$, and the operational signature.

The type signature gives each constant $\hat{a}$ and automaton state $\hat{q}$ kinds `Val` and `State` respectively. Furthermore, for each protected function f, the type signature specifies a predicate δ_f. The invariant the type system ensures is that for all $\hat{q_1},\hat{q_2},\hat{a}_1,\ldots,\hat{a}_n$, we will be able to prove the predicate $\delta_f(\hat{q_1},\hat{q_2},\hat{a}_1,\ldots,\hat{a}_n)$ only if the corresponding automaton transition holds. In other words, only if $\delta(f)(q_1,a_1,\ldots,a_n)=q_2$

The value signature specifies that objects a and states q are given the correct singleton types. For each protected function f in the source language, the target language contains two functions. The function δ_f is supplied by the implementer of the security policy; it is used to dynamically determine the automaton state transition function given the program executes the function f in the state ϱ_1 with arguments identified by $\rho_1,\ldots,\rho_n$. When δ_f has computed the transition, it calls its continuation, passing it the next state ϱ_2 so the continuation can test this state to determine whether it is *bad*. The continuation assumes the predicate $\delta_f(\varrho_1,\varrho_2,\rho_1,\ldots,\rho_n)$. Before calling the function f itself, we require that the type-checker be able to prove that f will make a transition to some state other than the bad state. Hence the precondition on f states that we must know the automaton transition that will occur $(\delta_f(\varrho_1,\varrho_2,\rho_1,\ldots,\rho_n))$ and moreover that the new state ϱ_2 is not equal to *bad*.

Now that we have fully defined the target language and specialized it for a particular security automaton, we can prove that the type system satisfies a number of properties. In the next section, we show the target language type syste is sound and enforces the security policy.

4.4 Properties of $\lambda_{\mathcal{A}}$

A predicate P is valid with respect to an automaton $\mathcal{A}$, written $\mathcal{A}\models P$, if:

- P is $\neq(\hat{q},\hat{q}')$ and $q\neq q'$, or
- P is $\delta_f(\hat{q}_1,\hat{q}_2,\hat{a}_1,\ldots,\hat{a}_n)$ and $\delta(f)(q_1,a_1,\ldots,a_n)=q_2$

We say that an expression e is *secure* with respect to a security automaton $\mathcal{A}$ in state q, written $\mathcal{A};q\vdash e$, if

1. $q\neq \mathit{bad}$

and there exist predicates $P_1,\ldots,P_n$ such that:

2. $\mathcal{A}\models P_i$, for $1\le i\le n$
3. $P_1,\ldots,P_n;\cdot;\hat{q}\vdash e$

If we can prove that an expression e is secure in our deductive system then the expression should not violate the security policy when it executes. The soundness theorem below formalizes this notion. The first part of the theorem, *Type Soundness*, ensures that programs obey a basic level of

$\boxed{\text{Type and Value Signature}}$

$$
\begin{array}{lcl}
\mathcal{I}(\hat{a}) & = & \texttt{Val} \qquad \text{for } a \in \mathrm{A} \\
\mathcal{I}(\hat{q}) & = & \texttt{State} \qquad \text{for } q \in Q \\
\\
\mathcal{I}(\delta_f) & = & (\texttt{State}, \texttt{State}, \overbrace{\texttt{Val}, \ldots, \texttt{Val}}^{n}) \rightarrow \mathcal{B} \\
 & & \quad \text{if } \mathcal{C}_{source}(f) = (b_1, \ldots, b_n, (b) \rightarrow 0) \rightarrow 0 \\
\\
\mathcal{C}(a) & = & b(\hat{a}) \qquad \text{if } \mathcal{C}_{source}(a) = b \\
\mathcal{C}(q) & = & \texttt{S}(\hat{q}) \qquad \text{if } q \in Q \\
\mathcal{C}(\delta_f) & = & \forall[\varrho_1{:}\texttt{State}, \rho_1{:}\texttt{Val}, \ldots, \rho_n{:}\texttt{Val}, \neq (\varrho_1, bad)].(\varrho_1, S(\varrho_1), b_1(\rho_1), \ldots, b_n(\rho_n), \\
 & & \quad \forall[\varrho_2{:}\texttt{State}, \delta_f(\varrho_1, \varrho_2, \rho_1, \ldots, \rho_n)](\varrho_1, S(\varrho_2)) \rightarrow 0) \rightarrow 0 \\
 & & \quad \text{if } \mathcal{C}_{source}(f) = (b_1, \ldots, b_n, (b) \rightarrow 0) \rightarrow 0 \\
\mathcal{C}(f) & = & \forall[\varrho_1{:}\texttt{State}, \varrho_2{:}\texttt{State}, \rho_1{:}\texttt{Val}, \ldots, \rho_n{:}\texttt{Val}, \neq (\varrho_2, bad), \delta_f(\varrho_1, \varrho_2, \rho_1, \ldots, \rho_n)]. \\
 & & \quad (\varrho_1, b_1(\rho_1), \ldots, b_n(\rho_n), \forall[].(\varrho_2, \exists\rho{:}\texttt{Val}.b(\rho)) \rightarrow 0) \rightarrow 0 \\
 & & \quad \text{if } \mathcal{C}_{source}(f) = (b_1, \ldots, b_n, (b) \rightarrow 0) \rightarrow 0
\end{array}
$$

$\boxed{\text{Operational Signature}}$

$$
\begin{array}{ll}
\delta_f[\hat{q_1}][\hat{a_1}] \cdots [\hat{a_n}][\cdot](q_1, a_1, \ldots, a_n, v_{cont}) & \text{if } \delta(f)(q_1, a_1, \ldots, a_n) = q_2 \\
\quad \longmapsto_{\cdot} v_{cont}[\hat{q_2}][\cdot](q_2) & \text{and for } 1 \leq i \leq n, \mathcal{C}_{source}(a_i) = b_i \\
 & \text{and } \mathcal{C}_{source}(f) = (b_1, \ldots, b_n, (b) \rightarrow 0) \rightarrow 0 \\
\\
f[\hat{q_1}][\hat{q_2}][\hat{a_1}] \cdots [\hat{a_n}][\cdot][\cdot](a_1, \ldots, a_n, v_{cont}) & \text{if for } 1 \leq i \leq n, \mathcal{C}_{source}(a_i) = b_i \\
\quad \longmapsto_{f(a_1, \ldots, a_n)} v_{cont}(\textbf{pack}[\hat{a}, a] \; as \; \exists\rho{:}\texttt{Val}.b(\rho)) & \text{and } \mathcal{C}_{source}(f) = (b_1, \ldots, b_n, (b) \rightarrow 0) \rightarrow 0 \\
\quad \text{(for some } a \text{ such that } \mathcal{C}_{source}(a) = b)
\end{array}
$$

Figure 8: Target Language Interface

control-flow safety. More specifically, it ensures that expressions do not get *stuck* during the course of evaluation. An expression e is *stuck* if e is not **halt** and there does not exist an e' such that $e \longmapsto_s e'$. Hence, Type Soundness implies a program will only halt when it executes the halt instruction and not because we have applied a function to too few or the wrong types of arguments. The second part of the theorem, *Security*, ensures programs obey the policy specified by the security automaton $\mathcal{A}$. In other words, the sequence of protected operations executed by the program must form a string in the language $\mathcal{L}(\mathcal{A})$. In this second statement, we use the notation $|s_1, \ldots, s_n|$ to denote the subsequence of the symbols $s_1, \ldots, s_n$ with all occurences of $\cdot$ removed.

Theorem 1 (Soundness)
If $\mathcal{A}; q_0 \vdash e_1$ *then*

1. (Type Soundness) *For all evaluation sequences* $e_1 \longmapsto_{s_1} e_2 \longmapsto_{s_2} \cdots \longmapsto_{s_n} e_{n+1}$*, the expression* e_{n+1} *is not* stuck.
2. (Security) *If* $e_1 \longmapsto_{s_1} e_2 \longmapsto_{s_2} \cdots \longmapsto_{s_n} e_{n+1}$ *then* $|s_1, s_2, \ldots, s_n| \in \mathcal{L}(\mathcal{A})$

Soundness can be proven syntactically in the style of Wright and Felleisen [30] using the following two lemmas. The proof appears in a companion technical report [29].

Lemma 2 (Progress) *If* $\mathcal{A}; q \vdash e$ *then either:*

1. $e \longmapsto_s e'$ *or*
2. $e = \textbf{halt}$

Lemma 3 (Subject Reduction) *If* $\mathcal{A}; q \vdash e$ *and* $e \longmapsto_s e'$ *then*

1. *if* $s = \cdot$ *then* $\mathcal{A}; q \vdash e'$
2. *and if* $s = f(a_1, \ldots, a_n)$ *then* $\mathcal{A}; q' \vdash e'$ *where* $\delta(f)(q, a_1, \ldots, a_n) = q'$

Finally, inspection of the typing rules will reveal that for any expression or value, there is exactly one typing rule that applies and that the preconditions for the rules only depend upon subcomponents of the terms or values (with possibly a predicate substitution). Judgements for the well-formedness of types and predicates are also well-founded so the type system is decidable:

Proposition 4 *It is decidable whether or not* $\Phi \vdash e$*.*

4.5 Language Extensions

If security policies depend upon higher-order functions or immutable data structures such as tuples and records, we will have to track the values of these data structures in the type system using singleton types as we did with values of base type. The simplest way to handle this extension is to use an allocation semantics (See, for example, [17]). In this setting, when a function closure $\texttt{fix}\, g[\Delta](\cdots).e$ is allocated, it is bound to a new address (ℓ). Instead of substituting the closure through the rest of the code as we do now, we would substitute the address (ℓ) through the code and give it the singleton type $\tau(\hat{\ell})$ where τ is $\forall[\Delta](\cdots) \rightarrow 0$. All the other mechanisms remain unchanged. For the sake of simplicity, we decided not to present this style of semantics.

There are a number of possibilities for handling mutable data structures. The main principle is that if security-sensitive operations depend upon mutable data then the

$$
\begin{array}{lcl}
|b| & = & \exists\rho{:}\mathtt{Val}.b(\rho) \\
|(\tau_1,\ldots,\tau_n)\to 0| & = & \forall[\varrho{:}\mathtt{State}, \neq(\varrho, bad)].(\varrho, \mathtt{S}(\varrho), |\tau_1|,\ldots,|\tau_n|)\to 0 \\
 & & \\
|x| & = & x \\
|a| & = & \mathtt{pack}[\hat{a}, a]\ \mathit{as}\ \exists\rho{:}\mathtt{Val}.b(\rho) \quad \text{if } \mathcal{C}_{source}(a) = b \\
|\mathtt{fix}\, g(x_1{:}\tau_1,\ldots,x_n{:}\tau_n).e| & = & \mathtt{fix}\, g[\varrho{:}\mathtt{State}, \neq(\varrho, bad)].(\varrho, x{:}S(\varrho), x_1{:}|\tau_1|,\ldots,x_n{:}|\tau_n|).|e|_{\varrho,x} \\
|f| & = & \mathtt{fix}\, \_[\varrho_1{:}\mathtt{State}, \neq(\varrho_1, bad)](\varrho_1, x_0{:}S(\varrho_1), x_1{:}|b_1|,\ldots,x_n{:}|b_n|, x_{n+1}{:}|(b)\to 0|). \\
 & & \qquad \mathtt{let}\, \rho_1, x_1' = \mathtt{unpack}\, x_1\, \mathtt{in} \\
 & & \qquad \ldots \\
 & & \qquad \mathtt{let}\, \rho_n, x_n' = \mathtt{unpack}\, x_n\, \mathtt{in} \\
 & & \qquad \mathtt{let}\, \varrho_2, \delta_f(\varrho_1,\varrho_2,\rho_1,\ldots,\rho_n), x_{\varrho_2} = \delta_f[\varrho_1][\rho_1]\cdots[\rho_n][\cdot](x_0, x_1',\ldots,x_n')\, \mathtt{in} \\
 & & \qquad \mathtt{if}\, x_{\varrho_2}(\\
 & & \qquad\qquad bad \to \mathtt{halt} \\
 & & \qquad\qquad |\ \_ \to \mathtt{let}\, x = f[\varrho_1][\varrho_2][\rho_1]\cdots[\rho_n][\cdot][\cdot](x_1',\ldots,x_n')\, \mathtt{in} \\
 & & \qquad\qquad\qquad x_{n+1}[\varrho_2][\cdot](x_{\varrho_2}, x)) \\
 & & \text{if } \mathcal{C}_{source}(f) = (b_1,\ldots,b_n,(b)\to 0)\to 0 \\
 & & \\
|v_0(v_1,\ldots,v_n)|_{P,v} & = & |v_0|[P][\cdot](v, |v_1|,\ldots,|v_n|) \\
|\mathtt{halt}\,|_{P,v} & = & \mathtt{halt}
\end{array}
$$

Figure 9: Program Instrumentation

$$
\begin{array}{llcl}
\mathit{types} & \tau & ::= & b \mid (\tau_1,\ldots,\tau_n)\to 0 \\
\mathit{constants} & a & \in & \mathrm{A} \\
\quad \mathit{protected\ ops} & f & \in & \mathrm{F} \\
\mathit{values} & v & ::= & x \mid a \mid f \mid \\
 & & & \mathtt{fix}\, g(x_1{:}\tau_1,\ldots,x_n{:}\tau_n).e \\
\mathit{expressions} & e & ::= & v_0(v_1,\ldots,v_n) \mid \mathtt{halt}
\end{array}
$$

Figure 10: Source Language Syntax

state of that data must be encoded in the state of the automaton. The assignment operator must be designated as a protected operation that changes the state.

5 Program Instrumentation

It is easy to design a translation that instruments a safe source language program with security checks now that we have set up the appropriate type-theoretic machinery in the target language. For the purposes of this paper, we will instrument programs written in a continuation-passing style simply-typed lambda calculus. The syntax of the language can be found in Figure 10. We will assume a static semantics given by judgements $\Gamma \vdash_{source} v : \tau$ and $\Gamma \vdash_{source} e$ where Γ is a finite map from value variables to types. Constants a and f are given types by the source signature $\mathcal{C}_{source}$ described in the previous section. Other than this, the semantics are entirely standard and have been omitted. Figure 9 gives the instrumentation algorithm in two parts: a type translation and a term translation. Here and in later section, we will use the abbreviation:

$$
\begin{array}{l}
\mathtt{let}\, \Delta, x_1,\ldots,x_n = v(v_1,\ldots,v_n)\, \mathtt{in}\, e \equiv \\
v(v_1,\ldots,v_n, \mathtt{fix}\, \_[\Delta].(x_1{:}\tau_1,\ldots,x_n{:}\tau_n).e)
\end{array}
$$

In the translation in Figure 9, we assume predicate and value variables bound by `let` are fresh.

The interesting portion of the type translation involves the translation of function types. The static semantics maintains the invariant that programs never enter the bad state and we naturally express this fact as a precondition to every function call. Hence the translation of $(\tau_1,\ldots,\tau_n)\to 0$ is $\forall[\varrho{:}\mathtt{State}, \neq(\varrho, bad)].(\varrho, \mathtt{S}(\varrho), |\tau_1|,\ldots,|\tau_n|)\to 0$. In general, we may not know the current state statically so we quantify over all states ϱ, provided $\varrho \neq bad$. In order to determine state transfers do not go wrong, we will also have to thread a representation of the state ($\mathtt{S}(\varrho)$) through the computation.

Every value of base type b is packed up as the existential $\exists\rho{:}\mathtt{Val}.b(\rho)$ so that it can be used generically in the normal case. In other words, wherever we used an integer in the source language, we will be able to use the target language type $\exists\rho{:}\mathtt{Val}.b(\rho)$. However, when we come to the translation of a protected operation, these generic values will be unpacked so the type system can maintain precise information about them. In fact, examining Figure 9, we can see that the first step in the translation of protected operations f is to unpack its arguments. Next, we use the function δ_f to determine the state transition that will occur if we execute f on these arguments. After checking to ensure we do not enter the bad state, we execute f itself passing it a continuation that executes in state ϱ_2.

Instrumented programs type check and thus they are *secure* in the sense made precise in the last section:

Proposition 5 *If* $\vdash_{source} e$ *then* $\mathcal{A}; q_0 \vdash |e|_{\hat{q_0},q_0}$.

This property can be proven using a straightforward induction on the typing derivation of the source term.

5.1 An Example: The Taxation Applet

In order to demonstrate the translation, we have written a simple "taxation applet" in the source language. When invoked, this applet sends a request out for tax forms. After sending the request, the applet reads a private file containing the customer salary before computing the taxes owed. We will assume files (*file*) and integers (*int*) are available as base types; *send* and *read* are the two protected operations:

```
fix _(secret:file, $x_{cont}$:(int) → 0).
  let _      = send() in          % send for tax forms
  let salary = read(secret) in    % read salary
let $taxes$ $= salary$ in          % compute taxes!!
$x_{cont}(taxes)$
```

The code below shows the results of instrumentating the taxation applet with checks from the simple file system security automaton of Section 3. We have simplified the output of the formal translation slightly to make it more readable. In particular, we have inlined the functions that the translation wraps around each protected operation. When reading the code calling *send* or *read*, notice that the instantiation of predicate variables indicates the state transition that occurs. For example, execution of the expression $send[\varrho_1][\varrho_2][\cdot][\cdot]()$ causes the automaton to make a transition from ϱ_1 to ϱ_2. When reading the checking functions, for example, $\delta_{send}[\varrho_1][\cdot](x_{\varrho_1})$, notice that we are checking the validity of the operation in the state indicated by the arguments (ϱ_1 and x_{ϱ_1}) and that the result is the next state.

```
fix _[$\varrho_1$:State, $\neq(\varrho_1, bad)$]
    $(\varrho_1, x_{\varrho_1}$:S$(\varrho_1), secret$:$\exists\rho$:Val.$file(\rho)$,
    $x_{cont}$:$\tau_{cont})$.
  let $\varrho_2, \delta_{send}(\varrho_1, \varrho_2), x_{\varrho_2} = \delta_{send}[\varrho_1][\cdot](x_{\varrho_1})$ in
  if $x_{\varrho_2}$ (
    $bad \rightarrow$ halt
    | _$\rightarrow$
      let _ $= send[\varrho_1][\varrho_2][\cdot][\cdot]()$ in
      let $\rho, secret'$ = unpack $secret$ in
      let $\varrho_3, \delta_{read}(\varrho_2, \varrho_3, \rho), x_{\varrho_3}$ =
        $\delta_{read}[\varrho_2][\cdot](x_{\varrho_2}, secret')$ in
      if $x_{\varrho_3}$ (
        $bad \rightarrow$ halt
        | _$\rightarrow$
          let $salary = read[\varrho_2][\varrho_3][\cdot][\cdot](secret')$ in
          let $taxes = salary$ in
          $x_{cont}[\varrho_3][\cdot](x_{\varrho_3}, taxes)$))
```

where τ_{cont} =
$\forall[\varrho_{cont}, \neq(\varrho_{cont}, bad)]$.
$(\varrho_{cont}, \mathtt{S}(\varrho_{cont}), \exists\rho'$:Val.$int(\rho')) \rightarrow 0$

The translation does not assume that the taxation applet is invoked in the initial automaton state and consequently the resulting function abstracts the input state ϱ_1. Also, as specified by the translation, objects of base type, like the file *secret* become existentials. The main point of interest in this example is that before each of the protected operations *send* and *read*, the corresponding automaton function determines the next state. Then the `if` construct checks that these states are not *bad*. In the successful branch, the type checker introduces information into the context that allows it to infer that executing the *read* and *send* operations is safe.

5.2 Optimization

Many security automata exhibit special structure that allows us to optimize secure programs by eliminating checks that are inserted by the naive program instrumentation procedure [27]. One common case is an operation f that always succeeds in a given state q and transfers control to a new state q' regardless of its arguments. In this situation, we can make the following axiom available to the type checker:

$$\frac{}{\Phi \vdash \delta_f(q, q', P_1, \ldots, P_n)} \text{ (for all } P_1, \ldots, P_n)$$

If we know we are in state q, we can use the axiom above and the fact that $q \neq bad$ to satisfy the precondition on f; there is no need to perform a run-time check.

The *send* operation in the security automaton in Section 3 has this property. When invoked in the initial state, *send* always succeeds and execution continues in the initial state. Therefore, we can safely add the axiom:

$$\frac{}{\Phi \vdash \delta_{send}(start, start)}$$

Now, if we know our taxation function is only invoked in the *start* state, we can rewrite it, eliminating one of the run-time checks:

```
% Optimization 1:
fix _[]$(start, x_{start}$:S$(start), secret$:$\exists\rho$:Val.$file(\rho)$,
      $x_{cont}$:$\tau_{cont})$.
  let _ $= send[start][start][\cdot][\cdot]()$ in
  ...
```

The type checker can prove *send* is executed in the *start* state and that the predicate $\delta_{send}(start, start)$ and the predicate $\neq(start, bad)$ are valid. Therefore, the optimized applet continues to type-check.

A second important way to optimize $\lambda_{\mathcal{A}}$ programs is to perform a control-flow analysis that propagates provable predicates statically through the program text. Using this technique, we can further optimize the taxation applet. Assume the calling context can prove the predicate $\delta_{read}(start, has\_read, \rho)$ (perhaps a run-time check was performed at some earlier time) where ρ is the value predicate corresponding to the file *secret*. In this case, the caller can invoke a tax applet with a stronger precondition that includes the predicate $\delta_{read}(start, has\_read, \rho)$. Moreover, with this additional information, an optimizer can eliminate the redundant check surrounding the file read operation:

```
% Optimization 2:
fix _[$\rho$:Val, $\delta_{read}(start, has\_read, \rho)$]$(start$,
      $secret$:$file(\rho)$,
      $x_{cont}$:$\forall[\,].(has\_read, \exists\rho$:Val.$int(\rho)) \rightarrow 0)$.
  let _ $= send[start][start][\cdot][\cdot]()$ in
  let $salary = read[start][has\_read][\cdot][\cdot](secret)$ in
  let $taxes = salary$ in
  $x_{cont}(taxes)$
```

In the code above, the optimizer rewrites the applet precondition with the necessary information. The caller is now obligated to prove the additional precondition before the applet can be invoked. The caller also unpacks the secret file before making the call so that the type checker can make the connection between the arguments to the δ_{read} predicate and this particular file. Finally, because the automaton state transitions are statically known throughout this program, we do not need to thread the state representation through the program. We assumed an optimizer was able to detect this unused argument and eliminate it. After performing all these optimizations, the resulting code is operationally equivalent to the original taxation applet from section 5.1, but provably secure.

The flexibility in the type system is particularly useful when a program repeatedly performs the same restricted operations. A more sophisticated tax applet might need to make a series of reads from the secret file (for charitable donations, number of dependents, etc.). If we assume the recursive function *read_a_lot* performs these additional reads, we need no additional security checks:

```
fix $read\_a\_lot$
    [$\varrho$:State, $\rho$:Val, $\delta_{read}(\varrho, has\_read, \rho), \neq(\varrho, bad)$]
    $(\varrho, secret{:}file(\rho),$
    $x_{cont}{:}\forall[\,](has\_read, \exists\rho{:}\texttt{Val}.int(\rho)) \to 0).$
% In unknown state $\varrho$
let $info = read[\varrho][has\_read][\cdot][\cdot]()$ in
% In known state $has\_read$
...
% Must prove $\delta(has\_read, has\_read, \rho)$
$read\_a\_lot[has\_read][\rho][\cdot][\cdot](secret, x_{cont})$
```

The *read_a_lot* function can be invoked in a good state ϱ (*i.e.* either *start* or *has_read*) when we can prove the predicate $\delta_{read}(\varrho, has\_read, \rho)$. Using the δ_{read} predicate in the function precondition, the type checker infers that the read operation transfers control from the ϱ state to the *has_read* state. Before the recursive call, the type checker has the obligation to prove $\delta_{read}(has\_read, has\_read, \rho)$ but it cannot do so because it only knows that $\delta_{read}(\varrho, has\_read, \rho)$! Fortunately, we can remedy this problem by adding another policy-specific rule to the type-checker:

$$\frac{\begin{array}{c}\Phi \vdash \neq (P, bad) \\ \Phi \vdash \delta_{read}(P, has\_read, P_f)\end{array}}{\Phi \vdash \delta_{read}(P', has\_read, P_f)} \quad \text{(for all } P, P', P_f)$$

This rule states that if we can read a file P_f in one state (P), then we can read it in any state (except the *bad* one) and we always move to the *has_read* state. This condition is easily decidable.

In practice, Erlingsson and Schneider's untyped optimizer analyzes security automaton structure and performs optimizations similar to the ones discussed above. Once the optimizer has obtained the information necessary for a particular transformation, this information can also be used to automatically generate the policy-specific axioms that we have discussed.

6 Related Work

The design of $\lambda_{\mathcal{A}}$ was inspired by Xi and Pfenning's Dependent ML (DML) [33, 31]. As in DML, we track the identity of values using dependent refinement types and singleton types. However, rather than applying the technology to array bounds check elimination and dead-code elimination, we have applied it to the problem of expressing security policies. Because their domain is different, Xi and Pfenning have not considered dependencies on the current state that are necessary here. On the other hand, they do consider existential dependent types of the form $\exists[\rho{:}\texttt{Val}, P(\rho)].\tau(\rho)$, which can be read "there exists a value ρ such that $P(\rho)$ and that ρ has type τ." Such existentials could be useful in a security setting. For example, they would allow users to manipulate collections of files that all have the property that they are readable or writeable. However, in order to take advantage of such types, a compiler would require very sophisticated type inference techniques or require application writers to annotate their code. Unlike Xi and Pfenning, one of the design goals of this work was to free application writers from the burden of having to write down additional information to prove properties of their programs. Therefore, because existentials of this form were not immediately necessary, we omitted them from the formalism.

Leroy and Rouaix [11] also consider security in the context of strongly-typed languages. Their main concern is proving that standard strongly-typed languages provide certain security properties. For example, they show that a program written in a typed lambda calculus augmented with references cannot modify unreachable (in the sense of tracing garbage collection) locations. They did not investigate mechanisms for mechanically checking that instrumented programs are safe, nor did they study the broader range of security policies that can be specified using security automata.

Several other systems use code instrumentation or other techniques to enforce safety properties. For instance, Evans and Twyman [2] have developed the Naccio system for specifying security policies. Like SASI, Naccio allows users to add security state to untrusted programs and to define operations that perform security checks. Sandholm and Schwartzbach [23] have developed a system for instrumenting concurrent programs to detect race conditions and violations of other safety properties. They take specifications in a second-order modal logic and compile them into a distributed security automaton. Godefroid [4] has a tool (VeriSoft) that detects violations of safety properties in concurrent programs using an extended model-checking technique. Fickas and Feather [3] have developed software that monitors properties of the environment that a process inhabits so that this information can be later used to help evolve the system. However, none of these other systems produce certified code and therefore they do not gain the benefits of redundant checking of their software; users must trust their compilers to do the right thing.

Acknowledgements

I am grateful to Úlfar Erlingsson and Fred Schneider for explaining their security automaton model and SASI system to me. Karl Crary, Úlfar Erlingsson, Neal Glew, Dan Grossman, Greg Morrisett, Stephanie Weirich, Steve Zdancewic, and the anonymous referees have made extremely helpful suggestions on previous drafts of this work.

References

[1] Karl Crary, Stephanie Weirich, and Greg Morrisett. Intensional polymorphism in type-erasure semantics. In *ACM International Conference on Functional Programming*, pages 301–312, Baltimore, September 1998.

[2] David Evans and Andrew Twyman. Flexible policy-directed code safety. In *IEEE Security and Privacy*, Oakland, May 1999.

[3] Stephen Fickas and Martin Feather. Requirements monitoring in dynamic environments. In *2nd IEEE International Symposium on Requirements Engineering*, March 1995.

[4] Patrice Godefroid. Model checking for programming languages using VeriSoft. In *Twenty-Fourth ACM Symposium on Principles of Programming Languages*, pages 174–186, Paris, January 1997.

[5] Robert Harper and Mark Lillibridge. A type-theoretic approach to higher-order modules with sharing. In *Twenty-First ACM Symposium on Principles of Programming Languages*, pages 188–201, Portland, Oregon, January 1994.

[6] Robert Harper and Greg Morrisett. Compiling polymorphism using intensional type analysis. In *Twenty-Second ACM Symposium on Principles of Programming Languages*, pages 130–141, San Francisco, January 1995.

[7] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[8] Dexter Kozen. Efficient code certification. Technical Report TR98-1661, Cornell University, January 1998.

[9] Christopher League, Zhong Shao, and Valery Trifonov. Representing java classes in a typed intermediate language. In *ACM International Conference on Functional Programming*, pages 183–196, Paris, January 1999.

[10] Xavier Leroy. Manifest types, modules, and separate compilation. In *Twenty-First ACM Symposium on Principles of Programming Languages*, pages 109 – 122, Portland, OR, January 1994.

[11] Xavier Leroy and Francois Rouaix. Security properties of typed applets. In *Twenty-Fifth ACM Symposium on Principles of Programming Languages*, pages 391–403, San Diego, January 1998.

[12] Tim Lindholm and Frank Yellin. *The Java Virtual Machine Specification.* Addison-Wesley, 1996.

[13] Y. Minamide, G. Morrisett, and R. Harper. Typed closure conversion. In *Twenty-Third ACM Symposium on Principles of Programming Languages*, pages 271–283, St. Petersburg, January 1996.

[14] John C. Mitchell and Gordon D. Plotkin. Abstract types have existential type. *ACM Transactions on Progamming Languages and Systems*, 10(3):470–502, July 1988.

[15] Greg Morrisett, Karl Crary, Neal Glew, Dan Grossman, Richard Samuels, Frederick Smith, David Walker, Stephanie Weirich, and Steve Zdancewic. TALx86: A realistic typed assembly language. In *ACM SIGPLAN Workshop on Compiler Support for System Software*, pages 25–35, Atlanta, GA, May 1999.

[16] Greg Morrisett, Karl Crary, Neal Glew, and David Walker. Stack-based typed assembly language. In *Second International Workshop on Types in Compilation*, pages 95–117, Kyoto, March 1998. Published in Xavier Leroy and Atsushi Ohori, editors, *Lecture Notes in Computer Science*, volume 1473, pages 28-52. Springer-Verlag, 1998.

[17] Greg Morrisett, Matthias Felleisen, and Robert Harper. Abstract models of memory management. In *ACM Conference on Functional Programming and Computer Architecture*, pages 66–77, La Jolla, June 1995.

[18] Greg Morrisett, David Walker, Karl Crary, and Neal Glew. From System F to Typed Assembly Language. *ACM Transactions on Progamming Languages and Systems*, 21(3):528–569, May 1999.

[19] George Necula. Proof-carrying code. In *Twenty-Fourth ACM Symposium on Principles of Programming Languages*, pages 106–119, Paris, 1997.

[20] George Necula and Peter Lee. Safe kernel extensions without run-time checking. In *Proceedings of Operating System Design and Implementation*, pages 229–243, Seattle, October 1996.

[21] George Necula and Peter Lee. The design and implementation of a certifying compiler. In *ACM Conference on Programming Language Design and Implementation*, pages 333 – 344, Montreal, June 1998.

[22] George C. Necula and Peter Lee. Safe, untrusted agents using proof-carrying code. *LNCS 1419: Special Issue on Mobile Agent Security*, October 1997.

[23] Anders Sandholm and Michael Schwartzbach. Distributed safety controllers for web services. In *Fundamental approaches to Software Engineering*, volume 1382, pages 270–284. Lecture Notes in Computer Science, Springer-Verlag, 1998.

[24] Fred Schneider. Enforceable security policies. Technical Report TR98-1664, Cornell University, January 1998.

[25] Chris Small. MiSFIT: A tool for constructing safe extensible C++ systems. In *Proceedings of the Third USENIX Conference on Object-Oriented Technologies*, Portland, OR, June 1997.

[26] Frederick Smith, David Walker, and Greg Morrisett. Alias types. Technical Report TR99-1773, Cornell University, October 1999.

[27] Úlfar Erlingsson and Fred B. Schneider. SASI enforcement of security policies: A retrospective. In *Proceedings of the 1999 New Security Paradigms Workshop*, Caledon Hills, September 1999.

[28] Robert Wahbe, Steven Lucco, Thomas Anderson, and Susan Graham. Efficient software-based fault isolation. In *Fourteenth ACM Symposium on Operating Systems Principles*, pages 203–216, Asheville, December 1993.

[29] David Walker. A type system for expressive security policies. Technical Report TR99-1740, Cornell University, April 1999.

[30] Andrew K. Wright and Matthias Felleisen. A syntactic approach to type soundness. *Information and Computation*, 115(1):38–94, 1994.

[31] Hongwei Xi. *Dependent Types in Practical Programming.* PhD thesis, Carnegie Mellon University, 1999.

[32] Hongwei Xi and Frank Pfenning. Eliminating array bound checking through dependent types. In *ACM Conference on Programming Language Design and Implementation*, pages 249–257, Montreal, Quebec, June 1998.

[33] Hongwei Xi and Frank Pfenning. Dependent types in practical programming. In *Twenty-Sixth ACM Symposium on Principles of Programming Languages*, pages 214–227, San Antonio, TX, January 1999.