

Policies

ANONYMOUS AUTHOR(S)

1 INTRODUCTION

Today's computing infrastructure is built atop layers of legacy C code, much of it distressingly insecure and difficult to maintain. These foundations need be shored up with additional security enforcement, but such mechanisms vary widely in their security goals and carry nuanced trade-offs between permissiveness and power. Enter Tagged C, a C variant with a built-in *tag-based reference monitor* that supports a range of user-defined security policies. Demonstrated in this paper: two varieties of *memory safety* exploring the trade-off between security and support for low-level idioms, *secure information flow* (SIF), and *compartmentalization*.

Legacy codebases, especially C codebases, pose a security conundrum. They are difficult to modify, the original programmers having moved on, so it may not be feasible to fix the bugs turned up by a conservative static analysis; a more permissive but unsound one, on the other hand, may miss bugs entirely. They may also contain undefined behavior (UB), possibly being used intentionally as a low-level idiom, while most static analyses treat UB as a failure. Where static analysis is unsatisfactory we turn to dynamic enforcement.

A tag-based reference monitor is a mechanism for dynamic security enforcement. It associates a metadata tag with the data in the underlying system, and throughout execution it updates these tags according to a set of predefined rules. If the program would violate a rule, the system halts instead, replacing a security violation with failstop behavior. By attaching such a monitor to the C language, we enable dynamic enforcement of arbitrary kinds of security, tuned so that non-standard but benign code can still run, while actually dangerous activity is failstopped.

This is the underlying concept of PIPE, an ISA extension that implements a reference monitor in hardware, as well as similar systems such as ARM MTE and [that thing from Binghamton]. Being implemented at the ISA level, these systems currently require their policies to be defined in terms of assembly code, usually with the help of a compiler. Instead, we attach tags to the C language itself, and aim to use PIPE as a compilation target, translating the high-level tags into PIPE's ISA primitives.

We offer the following contributions:

- A full formal semantics for Tagged C, formalized in Coq
- Proposed *control points* at which the language interfaces with the policy
- A Tagged C interpreter, implemented in Coq and extracted to Ocaml
- Policies implementing (1) realistic, permissive memory models from the literature (PVI and PNVI), (2) Secure Information Flow (SIF), and (3) compartmentalization

In the next section, we give a full account of the formal semantics of Tagged C, including its control points. Then in section 4, we describe how we attach a memory safety policy to it, in the process giving some justification of how we chose to attach the control points. In section 5, we give a similar description of a secure information flow policy. We round out our policies in section 6 with a compartmentalization policy. In ?? we discuss the degree to which the design meets our goals of flexibility and applicability to realistic security concerns.

1.1 Background

Exploits. [Talk about how there are a lot of exploits, they're problems, etc.]

2018. 2475-1421/2018/1-ART1 \$15.00
<https://doi.org/>

Reference Monitors. The concept of a reference monitor was first introduced fifty years ago in ??: a tamper-proof and verifiable subsystem that checks every security-relevant operation in a system to ensure that it conforms to a security *policy* (a general specification of acceptable behavior; see ??.)

A reference monitor can be implemented at any level of a system. An *inline reference monitor* is a purely compiler-based system that inserts checks at appropriate places in the code. Alternatively, a reference monitor might be embedded in the operating system, or in an interpreted language's runtime. A *hardware reference monitor* instead provides primitives at the ISA-level that accelerate security and make it harder to subvert.

Programmable Interlocks for Policy Enforcement (PIPE) [?] is a hardware extension that uses *metadata tagging*. Each register and each word of memory is associated with an additional array of bits called a tag. The policy is decomposed into a set of *tag rules* that act in parallel with each executing instruction, using the tags on its operands to decide whether the instruction is legal and, if so, determine which tags to place on its results. PIPE tags are large relative to other tag-based hardware, giving it the flexibility to implement complex policies with structured tags, and even run multiple policies at once.

Other hardware monitors include Arm MTE, [Binghamton], and CHERI. Arm MTE aims to enforce a narrow form of memory safety using 4-bit tags, which distinguish adjacent objects in memory from one another, preventing buffer overflows, but not necessarily other memory violations. [TODO: read the Binghamton paper, figure out where they sit here.]

CHERI is capability machine [TODO: cite OG CHERI]. In CHERI, capabilities are “fat pointers” carrying extra bounds and permission information, and capability-protected memory can only be accessed via a capability with the appropriate privilege. This is a natural way to enforce spatial memory safety, and techniques have been demonstrated for enforcing temporal safety [?], stack safety [?], and compartmentalization [TODO: figure out what to cite], with varying degrees of ease and efficiency. But CHERI cannot easily enforce notions of security based on dataflow, such as Secure Information Flow.

In this paper, we describe a programming language with an abstract reference monitor. We realize it as an interpreter with the reference monitor built in, and envision eventually compiling to PIPE-equipped hardware. An inlining compiler would also be plausible. As a result of this choice, our abstract reference monitor uses a PIPE-esque notion of tags.

PIPE Backend Implementation. In ??, Chhak et al. introduce a verified compiler from a toy high-level language with tags to a control-flow-graph-based intermediate representation with a PIPE-based ISA. This establishes a proof-of-concept for compiling a source language's tag policy to realistic hardware. They take advantage of the fact that, like everything else in a PIPE system, instructions in memory carry tags. Instruction tags are statically determined at compile-time. They “piggyback” information about source-level control points onto the tags of the instructions that implement those source constructs.

Tagged C is designed to be implemented in the same way. But, before we can soundly transmit tag rules from the source language to the assembly level, we also need to protect the basic control-flow properties of the source language. So, a compiled Tagged C requires a backend that can at the very least protect its control flow. In the case of a PIPE-based backend, we would run a basic stack-and-function-pointer-safety policy in parallel with whatever Tagged C policy the user has provided.

99	$\odot = !$		
100	\sim		
101	$-$	$\oplus ::= +$	Value
102	abs	\ll	Variable
103	$\odot ::= !$	$-$	\gg
104	\sim	\times	$\&$
105	$-$	\div	$ $
106	abs	$\%$	\wedge
107		$EaddrOf\ e$	Address of Object
108	$s ::= Sskip$	$Eunop\ \odot\ e$	Unary Operator
109	$Sdo\ e$	$Ebinop\ \oplus\ e_1\ e_2$	Binary Operator
110	$Sseq\ s_1\ s_2$	$Ecast\ ty\ e$	Cast
111	$Sif(e)\ then\ s_1\ else\ s_2\ join\ L$	$Econd\ e_1\ e_2\ e_3$	Conditional
112	$Swhile(e)\ do\ s\ join\ L$	$Esize(ty)$	Size of Type
113	$Sdo\ s\ while\ (e)\ join\ L$	$Ealign(ty)$	Alignment of Type
114	$Sfor(s_1; e; s_2)\ do\ s_3\ join$	$Eassign\ e_1\ e_2$	Assignment
115	$Sbreak$	$EassignOp\ \oplus\ e_1\ e_2$	Operator Assignment
116	$Scontinue$	$EpostInc\ \oplus\ e$	Post-Increment/Decrement
117	$Sreturn$	$Ecomma\ e_1\ e_2$	Expression Sequence
118	$Sswitch\ e\ \{ \overline{(L, s)} \}$	$Ecall\ ef\ \bar{e}_{args}$	Function Call
119	$Slabel\ L : s$	$Eloc\ l@lt$	Memory Location
120	$Sgoto\ L$	$Eparen\ e\ ty$	Parenthetical Cast
121			
122			
123			
124			
125			
126			
127			
128			
129			
130			
131			
132			
133			
134			
135			
136			
137			
138			
139			
140			
141			
142			
143			
144			
145			
146			
147			

Fig. 1. Tagged C Abstract Syntax

2 THE LANGUAGE

Tagged C uses full C syntax with minimal modification (fig. 1), but its semantics differ in two key respects. First, there is no memory-undefined behavior: the source semantics reflect a concrete target-level view of memory as a flat address space. Without memory safety, programs that exhibit memory-undefined behavior will act as their compiled equivalents would, potentially corrupting memory; we expect that a memory safety policy will be a standard default, but that the strictness of the policy may need to be tuned for programs that use low-level idioms.

Secondly, and more crucially, Tagged C's semantics contain *control points*: hooks within the operational semantics at which the tag policy is consulted and either tags are updated, or the system failstops. Control points resemble “advice points” in aspect-oriented programming, but narrowly focused on the manipulation of tags. A control point consists of the name of a *tag rule* and the bindings of its inputs and outputs; a tag rule is a partial function. The names and signatures of the tag rules, and their corresponding control points, are listed in Section 2.

The choice of control points and their associations with tag rules, as well as the tag rules' signatures, are a crucial design element. Our proposed design is sufficient for the three classes of policy that we explore in this paper, but it may not be complete.

Name	Inputs	Outputs	Control Points
GlobalT	$id \in ident, s \in \mathbb{N}$	pt, vt, \bar{lt}	Program initialization
LocalT	$\mathcal{P}, id \in ident, s \in \mathbb{N}$	pt, vt, \bar{lt}	Call
LoadT	$\mathcal{P}, pt, vt, \bar{lt}$	vt'	ValOf, AssignOp, PostIncr
StoreT	$\mathcal{P}, pt, vt_1, vt_2, \bar{lt}$	$\mathcal{P}', vt', \bar{lt}'$	Assign
ConstT		vt	Const, PostIncr
UnopT	\mathcal{P}, vt	vt	UnOp
BinopT	\mathcal{P}, vt_1, vt_2	vt'	BinOp
MallocT	\mathcal{P}, vt	$\mathcal{P}', pt, \boxed{vt, \bar{lt}}$	Call to malloc
FreeT	\mathcal{P}, vt	$\mathcal{P}', pt, \boxed{vt, \bar{lt}}$	Call to free
PICastT	$\mathcal{P}, pt, \boxed{vt, \bar{lt}}$	\mathcal{P}', vt	Cast from pointer to scalar
IPCastT	$\mathcal{P}, vt_1, \boxed{vt_2, \bar{lt}}$	\mathcal{P}', pt	Cast from scalar to pointer
PPCastT	$\mathcal{P}, pt, \boxed{vt, \bar{lt}}$	\mathcal{P}', pt'	Cast between pointers
IICastT	\mathcal{P}, vt_1	\mathcal{P}', pt	Cast between scalars
SplitT	$\mathcal{P}, vt, \boxed{L}$	\mathcal{P}'	Split points (??)
JointT	\mathcal{P}, \boxed{L}	\mathcal{P}'	Label
ArgT	\mathcal{P}, vt, f, x	vt'	Call
CallerRetT	$\mathcal{P}, \mathcal{P}', vt$	vt'	Return
CalleeRetT	$\mathcal{P}, \mathcal{P}', vt$	vt'	Return

3 FORMAL SEMANTICS

Tagged C uses a small-step reduction semantics, given in full in the appendix. We will introduce a limited set of step rules as they become relevant.

Values are ranged over by v , variable identifiers by x , and function identifiers by f . Tags use a number of metavariables: t ranges over all tags, while we will use vt to refer to the tags associated with values, pt for tags on pointer values and memory-location expressions, lt for tags associated with memory locations themselves, nt for “name tags” automatically derived from identifiers, and \mathcal{P} for the global “program counter tag” or PC Tag. An *atom* is a pair of a value and a tag, *Eval* $v@vt$; the @ symbol should be read as a pair in general, and is used when the second object in the pair is a tag. Expressions are ranged over by e (Figure 1), statements by s , and continuations by k . The continuations are defined in appendix A, and step rules in appendix B.

Global environments, ranged over by ge , map identifiers to either function or global variable definitions (including the variable’s location in memory. Local environments, ranged over by le , map identifiers to atoms. Memories m map integers to triples: a value, a “value tag” vt , and a list of “location tags” \bar{lt} .

A memory is an array of bytes, and a load or store will access some number of bytes. We write $m[l]_s = v@vt@\bar{lt}$ to denote loading s bytes, starting at location l , and interpreting them as a value v , a value tag vt , and a list of s location tags. Likewise, $m[l \mapsto v@vt@\bar{lt}]_s$ denotes storing that many bytes. vt is tied to a full value, which may consist of multiple bytes, while each tag in \bar{lt} is tied to an individual byte. When writing multiple contiguous values, we will write a range of locations. So in the case of an array of 10 integers, s would be 4, and $m[l \dots l + 10 \mapsto v@vt@\bar{lt}]_4$ would write $v@vt$ to ten words starting at l , with the four bytes of each word tagged with \bar{lt} ’s four

tags. This guarantees that even misaligned loads and stores always have a valid location tag to check (possibly multiple, mismatched location tags, in which case the policy can failstop if needed.)

States can be of several kinds, denoted by their script prefix: a *general state* $S(\dots)$, an *expression state* $\mathcal{E}(\dots)$, a *call state* $C(\dots)$, or a *return state* $\mathcal{R}(\dots)$. Finally, the special state *failstop* ($\mathcal{F}(\dots)$) represents a tag failure, and carries the state that produced the failure.

$$\begin{aligned} S ::= & S(m \mid s \gg k@P) \\ & | \mathcal{E}(m \mid e \gg k@P) \\ & | C(f, m, le \mid f'(\overline{Eval\ v@vt}) \gg k@P) \\ & | \mathcal{R}(m, ge, le \mid Eval\ v@vt \gg k@P) \\ & | \mathcal{F}(S) \end{aligned}$$

Expressions (??) use a contextual semantics; a call expression stores the context in the continuation all with the caller's continuation.

4 TAGS AND POLICIES

[TODO: consider moving control point discussion here]

Tagged C can enforce a wide range of policies, as follows. A policy consists of a tag type, a default tag inhabiting that type, and an instantiation of each tag rule identified in section 2.

Realizing the Policy. For each policy under discussion, we will give a code example of the sort of security situation in which it might be useful. We will introduce a formal characterization drawn from the literature of a security property that a correct policy should satisfy. [TODO: talk about properties somewhere before this?] Then we will walk through the important tag rules, and the control points that call them, introducing step rules as needed. Finally, if there are any implementation details that are necessary to realize a policy, we discuss those.

Control Points with Side-effects and Optional Arguments. Chhak et al. [?] give a general strategy for mapping Tagged C's tag rules onto instructions in a PIPE target. But as they note, translating tag rules in full generality requires adding extra instructions that may be unnecessary for some policies. The most problematic situation is when a Tagged-C control point requires a tag from a location that is not read under a normal compilation scheme or must update tags in locations that would otherwise not be written.

To mitigate this, control points whose compilation would add potentially extraneous instructions take optional parameters or return optional results. We will explain how the rule should be implemented in the target if the options are used. If a policy does not make use of the options, it will be sound to compile without the extra instructions. Optional inputs and outputs are marked with boxes.

Name Tags. When we want to define a per-program policy, we need to be able to attach tags to the program's functions, globals, and so on. We do this by automatically embedding their identifiers in tags, which are available to all policies. These are called *name tags* and are ranged over by nt . We give name tags to:

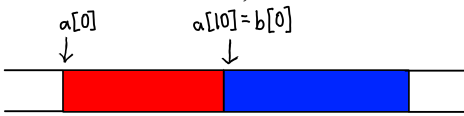
- Function identifiers
- Function arguments, written $f.x$
- Local and global variables
- Labels

4.1 Enforcing Memory Safety

Memory safety policies operate on under a “lock and key” model, in which objects in memory are tagged with a unique identifier (the “lock”) and may only be accessed via a pointer tagged with the same identifier (the “key.”) For a simple example, consider the following code:

```
void main() {
    int a[10];
    int b[10];
    a[10] = 42;
}
```

In a typical stack allocator—such as the one used by my interpreter—a and b will be allocated next to one another on the stack, like this:



To prevent the expression $a[10] = 42$ from overwriting $b[0]$, we give a and b unique *color tags* when they are allocated. In this case, we’ll tag a with *dyn 0*, indicating that it’s the first dynamically allocated object, and b with *dyn 1*. Then, when we evaluate the left-hand expression a into its memory location l , we tag l with *dyn 0*. When we take the offset $l + 10$, we keep that tag. And when we perform the assignment, we check that the location tag at l matches. It doesn’t, so we failstop.

The same principle applies for this code:

```
void main() {
    int* a = malloc(10 * sizeof(int));
    int* b = malloc(10 * sizeof(int));
    *(a + (b - a)) = 42;
}
```

In this case, a and b could be allocated anywhere in the heap, and in Tagged C the expression $*(a + (b - a)) = 42$ will always write to $*b$. While this might be intentional on the part of the programmer, it is also undefined behavior in the C standard, and in some (but not all; see below) formal C semantics. Likewise, if a and b are next to each other or in some other predictable arrangement, arithmetic like our first example can apply. The memory safety policy works just the same in this scenario, with the tags being attached by the call to malloc, once again using the *dyn* label in a global count of allocated blocks. Meanwhile, values that are not derived from valid pointers at all are tagged *X*, and can never be read or written through, to avoid pointer forging, like this:

```
void main() {
    int* a = malloc(10 * sizeof(int));
    // We happen to know that a will be at address 1000
    *1000 = 42;
}
```

Both stack and heap allocations use the *dyn* label and have a color that can grow arbitrarily high. This is because over a program’s execution, it might allocate an unbounded number of heap- or stack-allocated objects, and each needs a unique identifier. Existing work has shown that in

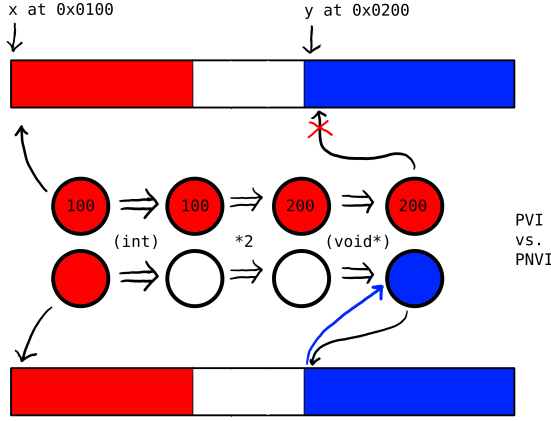


Fig. 2. Integer-pointer casts in PVI and PNVI

practice, tag colors can be “garbage collected” and reused, but in Tagged C we assume them to be infinite and unique.

Lastly, we have global variables. While “global safety” is not as prominent a topic as heap or stack safety, overrunning a global buffer is still a problem. It is also easy to forge a pointer to a global, and when this happens it can undermine assumptions about the behavior of linked libraries whose globals are not exported. Globals do not need dynamic colors, but can use their identifiers as tags, of the form *glob id*.

Memory Safety: PVI and PNVI. Our policies aim to enforce two memory models in particular: *PVI* (provenance via integer) and *PNVI* (provenance not via integer) from Memarian et al. [?]. They propose PVI and PNVI as memory models that support common idioms that are undefined in the C standard, but are still restrictive enough as to support useful alias analysis for optimization. This application is orthogonal to security, and violations of either memory model are treated as undefined behavior, just as in the C standard. Our goal is to turn that UB into failstop behavior, so that undefined programs cannot accidentally undermine their own security.

Both memory models represent pointers as integers, just as Tagged C does, with additional provenance associated with each object. An integer cast to a pointer in PVI retains this provenance, enabling integer operations to be performed on it prior to it being cast back to a pointer. In PNVI, by contrast, an integer cast to a pointer gains the provenance of the object it points to when the cast occurs. While PNVI supports a wider range of programs, it is inconsistent with important assumptions of the C memory model, in ways that may have serious security consequences. The difference between PVI and PNVI is illustrated in Figure 2.

We will aim to prove that for any program, if it is run in both the PVI semantics and in Tagged C with our PVI policy, it either produces identical output, or it is both undefined in the PVI semantics and failstops in Tagged C. Likewise for PNVI, except that some UB in PNVI is non-deterministic, and we only require that it failstop in an execution that would *reach* the UB.

4.2 PVI Definitions

Here we give the relevant tag rules for the PVI policy, and describe the control points that they attach to. We will, for each rule, first give the control point(s) that use it, along with a brief explanation

of what the surrounding semantics rules do, and then give the rule. For these policies, all control points appear in expression reduction steps. The machine state consists of the PC tag \mathcal{P} , a memory m , the global environment ge , and a local environment le . These are contextual semantics, so each expression is situated in some context ctx .

The core of the PVI policy is the *provenance color*, represented by a natural number.

$$\begin{array}{ll} T ::= glob\ id & id \in ident \\ dyn\ C & C \in \mathbb{N} \end{array}$$

Color generation. New colors are generated when objects are allocated. When exactly that occurs depends on where the object lives. Global variables are a special case: they are allocated during program initialization, before execution begins. As such they do not have a control point per se, but a rule that functions similarly, while being more expressive.

Given a list xs of variable identifiers id and types ty , a program's initial memory is defined by iteratively allocating each one in memory and updating the global environment with its base address, bound, type, and a static identity tag. Let $|ty|$ be a function from types to their sizes in bytes. The memory is initialized $undef@vt@lt$ for some vt and lt , unless given an initializer. Let m_0 and ge_0 be the initial (empty) memory and environment. The parameter b marks the start of the global region.

$$globals\ xs\ b = \begin{cases} (m_0, ge_0) & \text{if } xs = \varepsilon \\ (m[p \dots p + |ty| \mapsto \mathbf{undef@vt@lt}]_{|ty|}, & \text{if } xs = (id, ty) :: xs' \\ ge[id \mapsto (p, p + |ty|, ty, pt)]) & \text{and } pt, vt, lt \leftarrow \mathbf{GlobalT}(id, s) \\ & \text{where } (m, ge) = globals\ xs' (b + |ty|) \end{cases}$$

$\mathbf{GlobalT}(id, s)$

$$\begin{array}{ll} pt \leftarrow & glob\ id \\ vt \leftarrow & X \\ \overline{lt} \leftarrow & [glob\ id \mid 0 \leq i < s] \end{array}$$

Stack-allocated locals are allocated at the start of a function call. Like a global environment, a local environment maps identifiers to base, bound, type, and tag. The rule is almost identical to allocation of globals, except that the stack allocator, *stack_alloc* will be more complex in order to support deallocation (in practice, it uses a normal stack structure and allocates and deallocates by increasing and decreasing a “stack pointer”).

Since allocations occur at runtime, the value and location tags that initialize the allocated memory are optional. They would be realized by initializing the entire allocated object at allocation-time, which adds linear overhead if the object was not otherwise being initialized.

$$locals\ xs\ m\ le = \begin{cases} (m, le) & \text{if } xs = \varepsilon \\ locals\ xs' m'' le' & \text{if } xs = (id, ty) :: xs' \\ & \text{where } (m', p) \leftarrow \mathbf{stack_alloc}\ |ty|\ m, \\ & m'' = m'[p \dots p + |ty| \mapsto \mathbf{undef@vt@lt}]_{|ty|}, \\ & pt, vt, \overline{lt} \leftarrow \mathbf{LocalT}(\mathcal{P}, id, s), \\ & \text{and } le' = le[id \mapsto (p, p + |ty|, ty, pt)] \end{cases}$$

In the tag rule, the PC Tag carries the “next” color to be assigned. We mark both the pointer tag (which is stored in the local environment) with that color, along with the location tags on the allocated memory. Then we increment the PC Tag to give the next allocation a unique color.

LocalT(\mathcal{P}, id, s)

$pt \leftarrow \text{dyn } \mathcal{P}$

$\boxed{vt} \leftarrow X$

$\boxed{\overline{lt}} \leftarrow [\text{dyn } \mathcal{P} \mid 0 \leq i < s]$

$\mathcal{P}' \leftarrow \mathcal{P} + 1$

Heap objects are the most interesting: they are allocated via calls to malloc. In Tagged C, malloc is modeled as an external call to a built-in, so this takes the form of a special case of that expression. Where *heap_alloc* is some allocation function (a parameter of the memory model) that takes a size and a memory and returns an address:

$$\frac{\mathcal{P}', pt, \boxed{vt, \overline{lt}} \leftarrow \text{MallocT}(\mathcal{P}, vt) \quad m', p \leftarrow \text{heap_alloc size } m \quad m'' = m' [p + i \mapsto (\text{undef}, vt, lt) \mid 0 \leq i < s]}{\mathcal{E}(m \mid ctx [\text{malloc}(\text{size}@t)] \gg k@P) \longrightarrow \mathcal{E}(m'' \mid ctx [\text{Eval } p@pt] \gg k@P')}$$

And the tag rule is identical to **LocalT**, except that it always treats the allocated object as an array of bytes (making the location tags are always identical.)

MallocT(\mathcal{P}, vt)

$pt \leftarrow \text{dyn } \mathcal{P}$

$\boxed{vt} \leftarrow X$

$\boxed{\overline{lt}} \leftarrow [\text{dyn } \mathcal{P}]$

$\mathcal{P}' \leftarrow \mathcal{P} + 1$

Color Checking. When we perform a memory load or store, we check that the pointer tag on the left hand of the assignment matches the location tag on all of the bytes being loaded or stored. For instance, in a normal *valof* expression, which accesses a left-hand value:

$$\frac{m[l]_{|ty|} = v@vt@\overline{lt} \quad vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \overline{lt})}{\mathcal{E}(m \mid ctx [\text{EvalOf } \text{Eloc } l@pt] \gg k@P) \longrightarrow \mathcal{E}(m \mid ctx [\text{Eval } v@vt'] \gg k@P)}$$

We want to both check that the pointer tag matches all of the location tags, and propagate the value tag on the value in memory alongside that value.

LoadT($\mathcal{P}, pt, vt, \overline{lt}$)

assert $\forall lt \in \overline{lt}. pt = lt$

$vt' \leftarrow vt$

There are two other expressions that load from memory, and which therefore invoke this same rule, *assignop* and *postincr*. Note that the C spec has the order of evaluation for *assignop* “unsequenced”; I follow CompCert in evaluating both the left and right completely before performing the load. Intuitively, assignment-with-an-operator is classed along with the standard assignment in the spec, so it is appropriate that it be ordered in the same way.

$$\frac{m[l]_{|ty|} = v_1 @ vt @ \bar{lt} \quad \oplus \in \{+, -, *, /, \%, <, >, \&, ^, |\} \quad vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \bar{lt}) \quad e = \text{Eassign Eloc } l @ pt \text{ Ebinop } \oplus \text{ Eval } v_1 @ vt' \text{ Eval } v_2 @ vt_2}{\mathcal{E}(m \mid ctx [\text{EassignOp } \oplus \text{ Eloc } l @ pt \text{ Eval } v_2 @ vt_2] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m \mid ctx [e] \gg k @ \mathcal{P})}$$

$$\frac{m[l] = v @ vt @ \bar{lt} \quad \oplus \in \{+, -\} \quad vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \bar{lt}) \quad vt \leftarrow \text{ConstT } e = \text{Ecomma Eassign Eloc } l @ pt \text{ Ebinop } \oplus \text{ Eval } v @ vt' \text{ 1@ConstT Eval } v @ vt'}{\mathcal{E}(m \mid ctx [\text{EpostInc } \oplus \text{ Eloc } l @ pt] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m \mid ctx [e] \gg k @ \mathcal{P})}$$

On the flip side, we store values to memory using the *assign* expression:

$$\frac{m[l]_{|ty|} = v_1 @ vt_1 @ \bar{lt} \quad m' = m[l \mapsto v_2 @ vt' @ \bar{lt}'] \quad \mathcal{P}', vt', \bar{lt}' \leftarrow \text{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \bar{lt})}{\mathcal{E}(m \mid ctx [\text{Eassign Eloc } l @ pt \text{ Eval } v_2 @ vt_2] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m' \mid ctx [\text{Eval } v_2 @ vt_2] \gg k @ \mathcal{P})}$$

As before, we check that the pointer tag matches the locations tags, and then propagate the value tag (ignoring and overwriting the original value tag.) In addition, we propagate the PC Tag.

$$\begin{aligned} & \text{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \bar{lt}) \\ & \text{assert } \forall lt \in \bar{lt}. pt = lt \\ & \mathcal{P}' \leftarrow \mathcal{P} \\ & vt' \leftarrow vt_2 \\ & \bar{lt}' \leftarrow \bar{lt} \end{aligned}$$

Color Propagation. When a value moves from one location to another, it carries the same tag. We already saw this in the load and store rules: they maintain the relationship between the pointer and its tag. Of note here is the **VarT** control point, which transmits the pointer tag from the environment onto the location expression. In this policy, it propagates the color unchanged.

$$\frac{le[id] = (l, _, pt, ty) \quad pt \leftarrow \text{VarT}(\mathcal{P}, vt)}{\mathcal{E}(m \mid ctx [\text{Evar id}] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m \mid ctx [\text{Eloc } l @ pt] \gg k @ \mathcal{P})}$$

Then the color is propagated via all unary operations and all binary operations where exactly one argument has a color. Performing an operation with two values with color tags (i.e., two cast pointers) clears the tag on the result. It can still be used as an integer, but if cast back to a pointer it will be invalid.

$$\frac{\langle \odot \rangle v = v' \quad vt' = \text{UnopT}(\mathcal{P}, vt) \mathcal{P} vt}{\mathcal{E}(m \mid ctx [\text{Eunop } \odot \text{ Eval } v @ vt] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m \mid ctx [\text{Eval } v' @ vt'] \gg k @ \mathcal{P})}$$

$$\frac{v_1 \langle \oplus \rangle v_2 = v' \quad vt' = \text{BinopT}(\mathcal{P}, vt_1, vt_2) \mathcal{P} vt_1 vt_2}{\mathcal{E}(m \mid ctx [\text{Ebinop } \oplus \text{ Eval } v_1 @ vt_1 \text{ Eval } v_2 @ vt_2] \gg k @ \mathcal{P}) \longrightarrow \mathcal{E}(m \mid ctx [\text{Eval } v' @ vt'] \gg k @ \mathcal{P})}$$

$$\begin{array}{ll} \text{UnopT}(\mathcal{P}, vt) & \text{BinopT}(\mathcal{P}, vt_1, vt_2) \\ \mathcal{P}' \leftarrow \mathcal{P} & \mathcal{P}' \leftarrow \mathcal{P} \\ vt' \leftarrow vt & vt' \leftarrow \text{case } (vt_1, vt_2) \text{ of} \\ & \quad \text{dyn } n, X \Rightarrow \text{dyn } n \\ & \quad \text{glob id}, X \Rightarrow \text{glob id} \\ & \quad X, t \Rightarrow t \end{array}$$

4.3 PNVI Definitions

In PNVI, the basic provenance model remains the same as PVI, so we can reuse most of the same rules. The primary difference is what happens when we cast a pointer to an integer. In PVI, tags are propagated as normal.

To support PNVI, we need the *cast* expression to update the tags of a pointer being cast to an integer and vice versa. We add two special-case steps to reflect this.

$$\frac{\boxed{m[p]_{|ty|} = _@vt_2@lt} \quad \mathcal{P}', vt \leftarrow \text{PCastT}(\mathcal{P}, pt, \boxed{vt, \overline{lt}})}{\mathcal{E}(m \mid \text{Ecast Eval } p@pt \text{ int} \gg k@P) \text{ ptr}(ty) \longrightarrow \mathcal{E}(m \mid \text{Eval } p@vt \gg k@P) \text{ int}}$$

$$\frac{\boxed{m[p]_{|ty|} = _@vt_2@lt} \quad \mathcal{P}', pt \leftarrow \text{IPCastT}(\mathcal{P}, vt_1, \boxed{vt_2, \overline{lt}})}{\mathcal{E}(m \mid \text{Ecast Eval } p@pt \text{ int} \gg k@P) \text{ ptr}(ty) \longrightarrow \mathcal{E}(m \mid \text{Eval } p@vt \gg k@P) \text{ int}}$$

For casting an integer to a pointer, we don't need the optional "peek" at the memory that it points to. We simply clear the tag on the resulting integer.

$$\begin{aligned} & \text{PCastT}(\mathcal{P}, pt, \boxed{vt, \overline{lt}}) \\ & \mathcal{P}' \leftarrow \mathcal{P} \\ & vt \leftarrow X \end{aligned}$$

On the other hand, when casting back to a pointer, we need to check the color of the object that it points to.

$$\begin{aligned} & \text{IPCastT}(\mathcal{P}, vt_1, \boxed{vt_2, \overline{lt}}) \\ & \text{assert } \exists t. \forall lt \in \overline{lt}. lt = t \wedge t \neq X \\ & \mathcal{P}' \leftarrow \mathcal{P} \\ & pt \leftarrow t \end{aligned}$$

Realizing the Integer-Pointer Cast. The pointer cast rules take as input the tags on the location pointed to by the argument being cast. This requires the compiler to add extra instructions to retrieve that tag. On RISC-V, the sequence would be as follows, assuming that `a0` contains the value being cast. The meaning of instruction tags will be explained below.

```
lw a1 a0 0 @ RETRIEVE
sub a1 a1 a1 @ L
add a0 a1 a0 @ IPCAST
```

In the underlying assembly, we use instruction tags to inform the low-level monitor of the purpose of each instruction. RETRIEVE indicates a special load whose job is retrieve value and location tags from a location in memory. When it sees a RETRIEVE tag, the monitor allows the load even if it should failstop under the Concrete C backstop policy. If the load should failstop, however, it is given a default tag rather than the tags on the memory. A legal load receives both the value and the location tags.

The L instruction tag simply denotes taking the left-operand's tag on the result of a binary operation. In this case both operations are identical, but we still need to pick one. Finally, the IPCAST tag declares that this instruction should mimic the Tagged-C-level rule.

4.4 Secure Information Flow

To motivate our next policy, let's consider an erroneous piece of code:

```

540 void sanitize(src, dst);
541 char* sql_query(char* query);
542
543 void get_data(char* name, char* buf, int field) {
544     // field: 1=address, 2=phone, default=astrological sign
545     char[10] name_san;
546     char[100] query;
547     sanitize(name, name_san);
548
549     switch(field) {
550         case 1:
551             sprintf(query, "select address where name =");
552             strncat(query, name_san, strlen(name_san));
553             break;
554         case 2:
555             sprintf(query, "select phone where name =");
556             strncat(query, name_san, strlen(name_san));
557             break;
558         default:
559             sprintf(query, "select sign where name =");
560             strncat(query, name, strlen(name)); // Oops!
561             break;
562     }
563
564     sprintf(buf, sql_query(query));
565     return;
566 }

```

This function sanitizes its input name, then appends the result to an appropriate SQL query, storing the result in buf. But, in the default case, the programmer has accidentally used the unsanitized string! This creates the opportunity for an SQL injection attack: a caller to this function could (presumably at the behest of an outside user) call it with field of 3 and name of “Bobby; drop table;”.

We model this as a form of *secure information flow* (SIF), a variant of *information flow control* (IFC), as described in the venerable Denning and Denning [Denning and Denning 1977]. Specifically, this is an *intransitive* SIF setting: we wish to allow name to influence the result of sanitize, naturally, and the result of sanitize to influence the value passed to sql_query, but we do not wish for name to influence sql_query directly.

SIF is specified by a set of flow rules between what we will term *sources* and *sinks*. A source σ can be an argument of a function, its return value, or a global. A sink ψ can additionally be the set of heap objects allocated by a given function. We write these as follows:

$\sigma ::= x$	Global	$\psi ::= x$	Global
$f(x)$	Argument x of f	$f(x)$	Argument x of f
$f.ret$	Return value of f	$f.ret$	Return value of f
		$f.m$	Memory owned by f

In classic SIF theory, we specify an *information flow policy* (IFPol)—not to be confused with a tag policy—as a relation $\cdot \rightsquigarrow \cdot \in \sigma \times \psi$. However, manually defining such a policy is challenging, especially in an intransitive setting. We envision the IFPol being initially stated in negative terms,

with the “no-flow” relation $\not\rightsquigarrow$. That is, we will assume by default that for any source σ and any sink ψ , $\sigma \rightsquigarrow \psi$, unless the user has explicitly declared the contrary.

So, in the above example, the user would declare that `name` $\not\rightsquigarrow$ `sql_query`. But, in the case of `sanitize`, we want it to be the case that `name` can flow to `sql_query` only via `sanitize`. We therefore need to allow the user to declare a *declassification* rule. In general we will write σ/σ' to indicate that σ' supersedes σ : if a value that has been influenced by σ influences σ' , we can safely ignore its history with σ . We may write $*/\sigma$ to say that σ declassifies anything.

For example, suppose that in the following code, we want to enforce a no-flow rule between the argument `x` of `f` and the global variable `z` (`f.x` $\not\rightsquigarrow$ `z`), and a declassification rule $*/g.a$.

```
int z;

int g(int a);

void f(int x, int y) {
    z = x;           // violation
    z = x + y;       // violation
    if(x) z = 1; else z = 0; // violation
    z = g(x);        // violation, unless f.x / g.a
}
```

The first three lines of `f` violate the no-flow relation by storing values derived from `x` into `z`. The third line is especially interesting: although `x` is not stored directly, the value that is stored is conditioned upon it, and can be used to deduce information about the original value. This is termed an *implicit flow*. Finally, in the last line, the value of `g(x)` depends on `x`, which is a violation unless it is subject to a declassification rule.

We can therefore define an IFPol as a set of rules of each kind:

$$I \subseteq \{\sigma \not\rightsquigarrow \psi \mid \sigma \neq \psi\} \cup \{\sigma/\sigma' \mid \sigma \neq \sigma'\}$$

We do not need to distinguish between rules that notionally represent “integrity” versus “confidentiality” concerns. The SQL injection example is an instance of integrity, ensuring that an input cannot influence data in an undesired way, but the same concept can be used to prevent data from influencing the program’s output inappropriately.

SIF, formally. We can characterize the protection offered by a SIF policy in terms of a *non-interference* property along the lines of Bay and Askarov []. We annotate our transitions with events α , each representing the transmission of a value through a source or sink—possibly several. We write the projection of data relevant to a particular source σ or sink ψ as $\pi_\sigma(\alpha)$ or $\pi_\psi(\alpha)$.

$$\alpha ::=$$

[TODO: add the relevant events to their transitions in the semantics.]

Now, we define the knowledge that an observer monitoring a particular sink can extrapolate about the state of the system as a whole, as a set of states that are consistent with the events it observes. Given some initial state S , this is precisely the set of other initial states that might produce the same trace (or an extension thereof) and that are equivalent.

$$\mathbf{K}(S, \bar{\alpha}, \sigma, \psi) \triangleq \{S' \mid S \sim_\sigma S' \wedge S' \hookrightarrow_\psi \bar{\alpha} \cdot \alpha\}$$

Then, absent any declassification rules, we can define non-interference as holding between σ and ψ if, for any states S_1 and S_2 such that $S_1 \xrightarrow{\bar{\alpha} \cdot \alpha} S_2$, $\mathbf{K}(S_2, \bar{\alpha} \cdot \alpha, \sigma, \psi) \supseteq \mathbf{K}(S_1, \bar{\alpha}, \sigma, \psi)$. That is, every world that was possible before α remains possible after.

In the presence of declassification, we add an exception for the case where α reflects an event that should indeed allow an observer to gain some information. We extend the above definition to talk about all of I .

$$NI_I \triangleq \forall S_1, S_2, \bar{\alpha}, \alpha. \begin{cases} \mathbf{K}(S_2, \bar{\alpha} \cdot \alpha, \sigma, \psi) \supseteq \mathbf{K}(S_1, \bar{\alpha}, \sigma, \psi) & \text{if } \sigma \not\rightsquigarrow \psi \in I \\ \mathbf{K}(S_2, \bar{\alpha} \cdot \alpha, \sigma, \psi) \supseteq \mathbf{K}(S_1, \bar{\alpha}, \sigma \sqcup \sigma', \psi) & \text{if } \sigma/\sigma' \in I \wedge \sigma' \rightsquigarrow \psi \in I \end{cases}$$

Tagging SIF. We track the influence of a particular source, or its “taint,” through the system in the form of tags on values. A value that is tagged *vtaint* $\bar{\sigma}$ has been influenced by all of the sources in $\bar{\sigma}$. We also define a set of tags that indicate that a particular function argument or the memory location of an object represents a sink that is the target of one or more no-flow rules. If a sink ψ is tagged *forbid* $\bar{\sigma}$, then for all $\sigma \in \bar{\sigma}$, $\sigma \not\rightsquigarrow \psi$ must be in our IFPol. Finally, the PC Tag must carry additional information: when the PC Tag is tainted, it must keep a record of the scope of the taint, in the form of a label. We will explain below how this scope is computed.

$$\begin{aligned} T ::= & \text{vtaint } \bar{\sigma} \\ & \text{forbid } \bar{\sigma} \\ & \text{pctaint } \overline{(L, \sigma)} \end{aligned}$$

We define four important operations on tags: *join* ($t_1 \sqcup t_2$), *bounded join* ($t_1[L \rightsquigarrow t_2]$), *minus* ($t_1 - t_2$), and *check* ($t_1 \models t_2$), all partial functions.

$$\begin{aligned} t_1 \sqcup t_2 &\triangleq \begin{cases} \text{vtaint } (\bar{\sigma}_1 \cup \bar{\sigma}_2) & \text{if } t_1 = \text{vtaint } \bar{\sigma}_1 \text{ and } t_2 = \text{vtaint } \bar{\sigma}_2 \\ \text{vtaint } (\bar{\sigma}_2 \cup \{\sigma \mid (L, \sigma) \in \overline{(L, \sigma)}_1\}) & \text{if } t_1 = \text{pctaint } \overline{(L, \sigma)}_1 \text{ and } t_2 = \text{vtaint } \bar{\sigma}_2 \\ \text{vtaint } (\bar{\sigma}_1 \cup \{\sigma \mid (L, \sigma) \in \overline{(L, \sigma)}_2\}) & \text{if } t_2 = \text{pctaint } \overline{(L, \sigma)}_2 \text{ and } t_1 = \text{vtaint } \bar{\sigma}_1 \\ \perp & \text{otherwise} \end{cases} \\ L \rightsquigarrow t_1 \sqcup t_2 &\triangleq \begin{cases} \text{pctaint } (\bar{\sigma}_1 \cup \bar{\sigma}_2) & \text{if } t_1 = \text{vtaint } \bar{\sigma}_1 \text{ and } t_2 = \text{vtaint } \bar{\sigma}_2 \\ \perp & \text{otherwise} \end{cases} \\ t - \sigma &\triangleq \begin{cases} \text{taint } (\bar{\sigma}' - \sigma) & \text{if } t = \text{taint } \bar{\sigma}' \\ \perp & \text{otherwise} \end{cases} \\ t_2 \models t_1 &\triangleq \begin{cases} \mathbf{t} & \text{if } t_1 = \text{taint } \bar{\sigma}_1, t_2 = \text{forbid } \bar{\sigma}_2, \text{ and } \bar{\sigma}_1 \cap \bar{\sigma}_2 = \emptyset \\ \mathbf{f} & \text{if } t_1 = \text{taint } \bar{\sigma}_1, t_2 = \text{forbid } \bar{\sigma}_2, \text{ and } \bar{\sigma}_1 \cap \bar{\sigma}_2 \neq \emptyset \\ \perp & \text{otherwise} \end{cases} \end{aligned}$$

Tainting and Checking Arguments and Returns. Now we can begin to give our policy, given an arbitrary IFPol I .

A function argument or return value can be either a source or a sink. So, when they are processed by the *call-state* and *return-state* rules, we must both check that the value being passed or returned is not tainted by a forbidden source, and then add the current source to its taint. The call-state rule executes at the beginning of a call, moving all of its arguments into the local environment, using the **ArgT** tag rule. The return-state rule executes after the call returns, inserting the result into the

$$\begin{array}{c}
\text{def}(f) = (xs, s) \\
\frac{le' = le[x \mapsto v@vt' \mid (x, v@vt) \leftarrow \text{zip}(xs, args), vt' \leftarrow \text{ArgT}(\mathcal{P}, vt, f, x)]}{C(f, m, ge \mid le(args) \gg k@P) \longrightarrow S(m \mid ge \gg le'@P) sk} \\
\frac{k = Kcall\ le'\ ctx\ k' \quad \mathcal{P}'', vt' \leftarrow \text{CallerRetT}(\mathcal{P}, \mathcal{P}', vt)}{\mathcal{R}(m, ge, le \mid Eval\ v@vt \gg k@P) \longrightarrow \mathcal{E}(m \mid ctx[Eval\ v@vt'] \gg k'@P')}
\end{array}$$

Fig. 3. Call and Return Steps

context saved in the continuation. The program counter on return and the result's tag are set by the **CallerRetT** tag rule. Both are given in fig. 3.

ArgT(\mathcal{P}, vt, f, x)

let $t := \text{forbid} \{ \sigma \mid \sigma \not\rightsquigarrow f(x) \in I \}$ in
 assert $t \models \mathcal{P} \sqcup vt$
 let $vt_1 := vt - \{ \sigma \mid \sigma / f(x) \in I \}$ in
 let $vt_2 := vt_1 \sqcup \text{tainted} \{ f(x) \}$ in

$vt' \leftarrow vt_2$

CallerRetT($\mathcal{P}, \mathcal{P}', vt$)

let $t := \text{forbid} \{ \sigma \mid \sigma \not\rightsquigarrow f.ret \in I \}$ in
 assert $t \models \mathcal{P} \sqcup vt$
 let $vt_1 := vt - \{ \sigma \mid \sigma / f.ret \in I \}$ in
 let $vt_2 := vt_1 \sqcup \text{tainted} \{ f.ret \}$ in

$vt' \leftarrow vt_2$

Global variables are also possible sources or sinks. In this case, we initialize their tags to carry this information.

GlobalT(id, s)

$pt \leftarrow \text{tainted } \emptyset$
 $vt \leftarrow \text{tainted } \{x\}$
 $\overline{lt} \leftarrow [\text{forbidden } \{ \sigma \mid x \not\rightsquigarrow \sigma \in I \}]$

Introducing Dynamic Sinks. One scenario that does not really match the others is when the sink is dynamically allocated memory. In this case, we need to tag the memory at allocation-time with the forbidden sources.

MallocT(\mathcal{P}, vt)

$pt \leftarrow \mathcal{P} \sqcup \text{tainted } \emptyset$
 $\boxed{vt} \leftarrow \text{tainted } \emptyset$
 $\boxed{\overline{lt}} \leftarrow [\text{forbidden } \{ \sigma \mid \sigma \not\rightsquigarrow f.m \}]$
 $\mathcal{P}' \leftarrow \mathcal{P} + 1$

Propagating Taint Through Expressions. It is simple enough to determine when a value is tainted: at a function call, all function arguments are tagged with their source identity, and the result of any expression is tagged with the union of the sources of its operands. If the expression involves a store or function call itself, we must check the taints on the value being stored or passed against the forbidden list of the target.

Unary and binary operations:

UnopT(\mathcal{P}, vt)

$vt' \leftarrow vt$

BinopT(\mathcal{P}, vt_1, vt_2)

$vt' \leftarrow vt_1 \sqcup vt_2$

Loads and stores:

$$\begin{array}{ll}
\text{LoadT}(\mathcal{P}, pt, vt, \bar{lt}) & \text{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \bar{lt}) \\
vt' \leftarrow \mathcal{P} \sqcup pt \sqcup vt & \text{assert } \forall lt \in \bar{lt}. lt \models \mathcal{P} \sqcup pt \sqcup vt_2 \\
& \mathcal{P}' \leftarrow \mathcal{P} \\
& vt' \leftarrow \mathcal{P} \sqcup pt \sqcup vt_2 \\
& \bar{lt}' \leftarrow \bar{lt}
\end{array}$$

Implicit Flows. Things become trickier when the program's control-flow itself can be tainted. This can occur in any of our semantics' steps that can produce different statements and continuations depending on the tainted value. At that point, any change to the machine state constitutes an information flow.

To be more specific, consider a statement that contains an expression, $s(e)$, such that when filled in with a tainted value:

$$S(m \mid sEval\ v_1@taint\ \sigma \gg k@P) \longrightarrow S(m_1 \mid s_1 \gg k_1@P_1)$$

while

$$S(m \mid sEval\ v_1@taint\ \sigma \gg k@P) \longrightarrow S(m_2 \mid s_2 \gg k_2@P_2)$$

and where $s_1 \neq s_2$ or $k_1 \neq k_2$. Taking either step should taint the program state itself! We represent this as a taint on the PC Tag. When the PC Tag is tainted, all stores to memory and all updates to environments must also be tainted until all branches eventually rejoin. We term the point at which it is safe to remove taint a *join point*. In terms of the program's control-flow graph, the join point of a branch is its immediate post-dominator.

In many simple programs, the join point of a conditional or loop is obvious: the point at which the chosen branch is complete, or the loop has ended. Such a simple example can be seen in fig. 4; `public1` must be tagged with the taint tag of `secret`, while it is safe to tag `public2` `X`, because that is after the join point, `J`. The same goes for fig. 5, because we are in a *termination-insensitive* setting \square . This means that we consider only terminating runs. So, we can guarantee that the post-dominator `J` of the while loop is reached.

But in the presence of unrestricted go-to statements, a join point may not be local—and sometimes may not exist within the function, assuming that we have not consolidated return points. Consider fig. 6, which uses go-to statements to create an approximation of an if-statement whose join-point is far removed from the for-loop. The label `J` now has nothing to do with the semantics of any particular statement.

Luckily this can still be determined statically from a function's full control-flow graph. So, to implement the policy, we must first transform our program by adding labels at the join point of each conditional. Every statement that branches carries an optional label indicating its corresponding join point. If it doesn't have such a label, that indicates that there is no join point within the function—once the PC Tag is tainted, it must remain so until a return.

When we step into a conditional or loop, we record its join point on the PC Tag, associated with the sources that are tainted. Then, when we reach the label, we will subtract its sources from the PC Tag at that time. This means that if multiple branches share a join point, their taints will be removed simultaneously.

$$\begin{array}{ll}
\text{SplitT}(\mathcal{P}, vt, \boxed{L}) & \text{JointT}(\mathcal{P}, \boxed{L}) \\
\mathcal{P}' \leftarrow \mathcal{P}[L \mapsto vt] & \text{assert } \mathcal{P} = \text{pctaint } \overline{(L, \sigma)} \\
& \mathcal{P}' \leftarrow \text{pctaint } \{(L', \sigma) \mid (L', \sigma) \in \overline{(L, \sigma)} \wedge L \neq L'\}
\end{array}$$

```

785 int f(bool secret) {
786     int public1, public2;
787
788     S: if (secret) {
789         b1: public1 = 1;
790     } else {
791         b2: public1 = 0;
792     }
793
794     J: public2 = 42;
795
796     return public2;
797 }

```

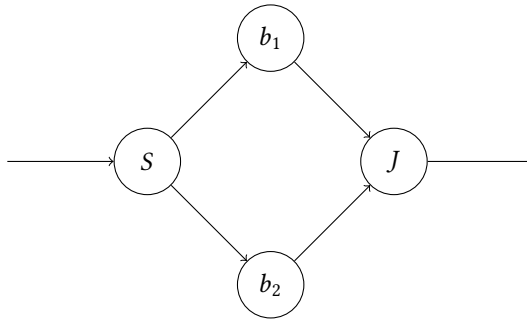


Fig. 4. Leaking via if statements

```

810 int f(bool secret) {
811     int public1=1;
812     int public2;
813
814     S: while (secret) {
815         b1: public1 = 1;
816         secret = false;
817     }
818
819     J: public2 = 42;
820
821     return public2;
822 }

```

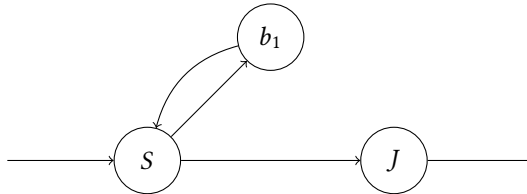


Fig. 5. Leaking via while statements

```

834 int f(bool secret) {
835     int public1, public2;
836
837     while (secret) {
838         goto b1;
839     }
840
841     b2: public1 = 1;
842     goto J;
843
844     b1: public1 = 1;
845
846     J: public2 = 42;
847     return public2;
848 }

```

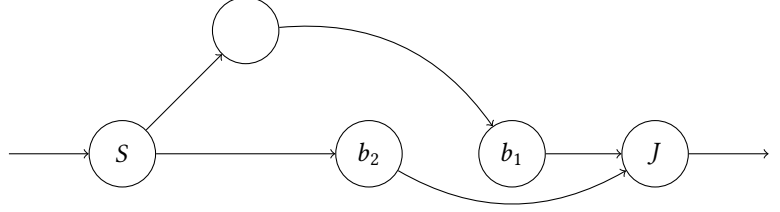


Fig. 6. Cheating with go-tos

$$\begin{array}{c}
 s' = \begin{cases} s_1 & \text{if } \text{boolof}(v) = t \\ s_2 & \text{if } \text{boolof}(v) = f \end{cases} \quad \mathcal{P}' \leftarrow \text{SplitT}(\mathcal{P}, vt, \boxed{L}) \\
 \hline
 \mathcal{E}(m \mid \text{Eval } v@vt \gg \text{Kif}[s_1 \mid s_2] \text{ join } L; k@P) \longrightarrow \mathcal{S}(m \mid s' \gg k@P') \\
 \hline
 \text{boolof}(v) = t \quad k_1 = \text{KwhileTest}(e) \{s\} \text{ join } L; k \quad k_2 = \text{KwhileLoop}(e) \{s\} \text{ join } L; k \\
 \hline
 \mathcal{E}(m \mid \text{Eval } v@vt \gg k_1@P) \longrightarrow \mathcal{S}(m \mid s \gg k_2@P') \\
 \hline
 \text{boolof}(v) = f \quad k = \text{KwhileTest}(e) \{s\} \text{ join } L; k' \\
 \hline
 \mathcal{E}(m \mid \text{Eval } v@vt \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P') \\
 \hline
 s = \text{Sskip} \vee s = \text{Scontinue} \quad k = \text{KwhileLoop}(e) \{s\} \text{ join } L; k' \\
 \hline
 \mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Swhile}(e) \text{ do } s \text{ join } L \gg k'@P) \\
 \hline
 k = \text{KwhileLoop}(e) \{s\} \text{ join } L; k' \\
 \hline
 \mathcal{S}(m \mid \text{Sbreak} \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P) \\
 \hline
 \mathcal{P}' \leftarrow \text{JointT}(\mathcal{P}, \boxed{L}) \\
 \hline
 \mathcal{S}(m \mid L : s \gg k@P) \longrightarrow \mathcal{S}(m \mid ge \gg le'@P') sk
 \end{array}$$

Fig. 7. Selected Conditional Steps

The **JointT** control point applies whenever we reach a labeled statement, seen in fig. 7. The remaining branching constructs are rather complicated, involving multiple steps and manipulations of the continuation that are not that relevant to their control points. Rather than give their semantics in full, it suffices to identify which transitions contain **SplitT** control points. In fig. 8, these are the transitions from the state marked *S*. Their semantics are given in full in the appendix.

Realizing IFC. In order to implement an IFC policy, we need to specify the rules that it needs to enforce. The positive here is that the rules are not dependent on one another (with the exception of declassification rules), and default to permissiveness when no rule is given. We assume that the user would supply a separate file consisting of a list of triples: the source, the sink, and the type of rule. This is then translated into the policy.

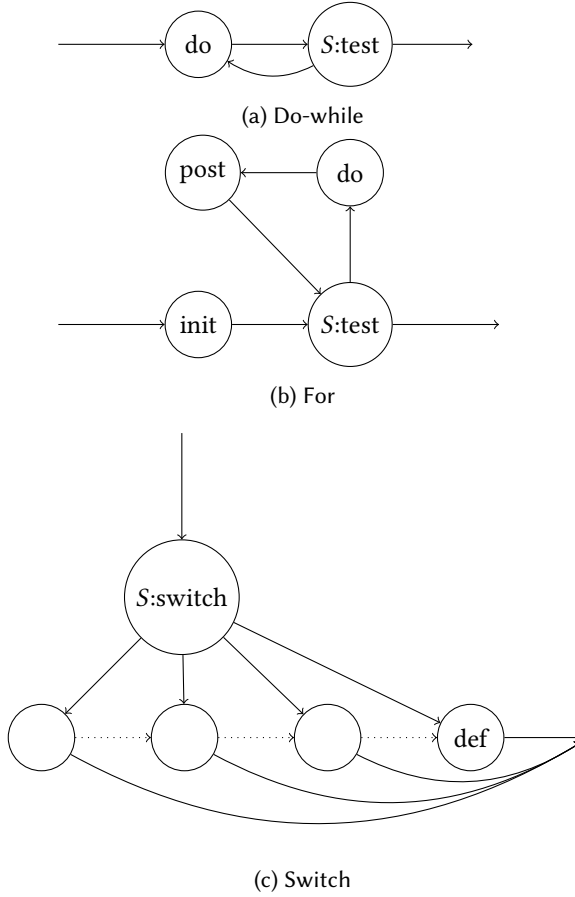


Fig. 8. Remaining Branch Statements

The other implementation detail to consider are the label tags. These resemble instruction tags, and that is exactly how they would be implemented: as a special instruction tag on the appropriate instruction, which might be an existing instruction or a specially added no-op. But importantly, in this case, these tags are mutable; in a policy that can be expected to take advantage of their mutability, we will need an extra store to set the tag for later.

It remains to generate those labels. For purposes of an IFC policy, we first generate the program's control flow graph. Then, for each if, while, do-while, for, and switch statement, we identify the immediate post-dominator in the graph, and wrap it in a label statement with a fresh identifier. That identifier is also added as a field in the original conditional statement. The tags associated with the labels are initialized at program state—in the case of IFC, these defaults declare that there are no secrets to lowre when it is reached.

4.5 Compartmentalization

Coverity has examples of: “all the old stuff goes over there, new code has stricter requirements.”

5 EVALUATION

Tagged C aims to combine the flexibility of tag-based architectures with the abstraction of a high-level language. How well have we achieved this aim?

[Here we list criteria and evaluate how we fulfilled them]

- Flexibility: we demonstrate three policies that can be used alone or in conjunction
- Applicability: we support the full complement of C language features and give definition to many undefined C programs
- Practical security: our example security policies are based on important security concepts from the literature

6 RELATED AND FUTURE WORK

Proofs.

REFERENCES

Dorothy E. Denning and Peter J. Denning. 1977. Certification of Programs for Secure Information Flow. *Commun. ACM* 20, 7 (jul 1977), 504–513. <https://doi.org/10.1145/359636.359712>

A CONTINUATIONS

$$\begin{aligned}
 k ::= & \text{Kemp} \\
 & | \text{Kdo}; k \\
 & | \text{Kseq } s; k \\
 & | \text{Kif}[s_1 \mid s_2] \text{ join } L; k \\
 & | \text{KwhileTest}(e) \{ s \} \text{ join } L; k \\
 & | \text{KwhileLoop}(e) \{ s \} \text{ join } L; k \\
 & | \text{KdoWhileTest}(e) \{ s \} \text{ join } L; k \\
 & | \text{KdoWhileLoop}(e) \{ s \} \text{ join } L; k \\
 & | \text{Kfor } s; k \\
 & | \text{KforPost } s; k
 \end{aligned}$$

B STEP RULES

B.1 Sequencing rules

$$\frac{}{S(m \mid e; \gg k@P) \longrightarrow E(m \mid e \gg Kdo; k@P)}$$

$$\frac{}{E(m \mid \text{Eval } v@vt \gg Kdo; k@P) \longrightarrow S(m \mid \text{Sskip} \gg k@P)}$$

$$\frac{}{S(m \mid s_1; s_2 \gg k@P) \longrightarrow S(m \mid s_1; \gg Kseq s_2; k@P)}$$

$$\frac{}{S(m \mid \text{Sskip} \gg Kseq s; k@P) \longrightarrow S(m \mid s \gg k@P)}$$

$$\frac{}{S(m \mid \text{Scontinue} \gg Kseq s; k@P) \longrightarrow S(m \mid \text{Scontinue} \gg k@P)}$$

$$\frac{}{S(m \mid \text{Sbreak} \gg Kseq s; k@P) \longrightarrow S(m \mid \text{Sbreak} \gg k@P)}$$

$$\begin{array}{c}
\text{pop } k = K\text{call } f' \text{ ctx } [] k' \\
\hline
\mathcal{S}(m \mid \text{Sreturn Eval } v@vt \gg k@P) \longrightarrow \mathcal{R}(P, m, ge \mid \text{Eval } v@vt \gg \text{ctx } [@] f') k \\
\hline
\mathcal{P}' \leftarrow \text{JointT}(P, \boxed{L}) \\
\hline
\mathcal{S}(m \mid L : s \gg k@P) \longrightarrow \mathcal{S}(m \mid ge \gg le'@P') sk
\end{array}$$

B.2 Conditional rules

$$\begin{array}{c}
s = \text{Sif}(e) \text{ then } s_1 \text{ else } s_2 \text{ join } L \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{E}(m \mid e \gg \text{Kif}[s_1 \mid s_2] \text{ join } L; k@P) \\
\hline
s' = \begin{cases} s_1 & \text{if } \text{boolof}(v) = \mathbf{t} \\ s_2 & \text{if } \text{boolof}(v) = \mathbf{f} \end{cases} \quad \mathcal{P}' \leftarrow \text{SplitT}(P, vt, \boxed{L}) \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg \text{Kif}[s_1 \mid s_2] \text{ join } L; k@P) \longrightarrow \mathcal{S}(m \mid s' \gg k@P')
\end{array}$$

TODO: switch

B.3 Loop rules

$$\begin{array}{c}
s = \text{Swhile}(e) \text{ do } s' \text{ join } L \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{E}(m \mid e \gg \text{KwhileTest}(e) \{ s \} \text{ join } L; k@P) \\
\hline
\text{boolof}(v) = \mathbf{t} \quad k_1 = \text{KwhileTest}(e) \{ s \} \text{ join } L; k \quad k_2 = \text{KwhileLoop}(e) \{ s \} \text{ join } L; k \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg k_1@P) \longrightarrow \mathcal{S}(m \mid s \gg k_2@P') \\
\hline
\text{boolof}(v) = \mathbf{f} \quad k = \text{KwhileTest}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P') \\
\hline
s = \text{Sskip} \vee s = \text{Scontinue} \quad k = \text{KwhileLoop}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Swhile}(e) \text{ do } s \text{ join } L \gg k'@P) \\
\hline
k = \text{KwhileLoop}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{S}(m \mid \text{Sbreak} \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P) \\
\hline
s = \text{Sdo } s \text{ while } (e) \text{ join } L \quad k' = \text{KdoWhileLoop}(e) \{ s \} \text{ join } L; k \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{S}(m \mid s \gg k'@P) \\
\hline
k_1 = \text{KdoWhileLoop}(e) \{ s \} \text{ join } L; k' \quad k_2 = \text{KdoWhileTest}(e) \{ s \} \text{ join } L; k \\
\hline
\mathcal{S}(m \mid s' = \text{Sskip} \vee s' = \text{Scontinue} \gg k_1@P) \longrightarrow \mathcal{E}(m \mid e \gg k_2@P) \\
\hline
\text{boolof}(v) = \mathbf{f} \quad k = \text{KdoWhileTest}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P') \\
\hline
\text{boolof}(v) = \mathbf{t} \quad k = \text{KdoWhileTest}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sdo } s \text{ while } (e) \text{ join } L \gg k'@P') \\
\hline
k = \text{KdoWhileLoop}(e) \{ s \} \text{ join } L; k' \\
\hline
\mathcal{S}(m \mid \text{Sbreak} \gg k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k'@P) \\
\hline
s = \text{Sfor}(s_1; e; s_2) \text{ do } s_3 \text{ join } L \quad s_1 \neq \text{Sskip} \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{S}(m \mid s_1 \gg \text{Kseq Sfor}(\text{Sskip}; e; s_2) \text{ do } s_3 \text{ join } L; k@P) \\
\hline
s = \text{Sfor}(\text{Sskip}; e; s_2) \text{ do } s_3 \text{ join } L \\
\hline
\mathcal{S}(m \mid s \gg k@P) \longrightarrow \mathcal{E}(m \mid e \gg \text{Kfor } s; k@P) \\
\hline
\text{boolof}(v) = \mathbf{f} \\
\hline
\mathcal{E}(m \mid \text{Eval } v@vt \gg \text{Kfor } s; k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k@P)
\end{array}$$

$$\begin{array}{c}
\frac{s = \text{Sfor}(\text{Sskip}; e; s_2) \text{ do } s_3 \text{ join } L \quad \text{boolof}(v) = \mathbf{t}}{\mathcal{E}(m \mid \text{Eval } v@vt \gg \text{Kfor } s; k@P) \longrightarrow \mathcal{S}(m \mid s_3 \gg \text{Kfor } s; k@P)} \\
\frac{s = \text{Sfor}(\text{Sskip}; e; s_1) \text{ do } s_2 \text{ join } L \quad s = \text{Sskip} \vee s = \text{Scontinue}}{\mathcal{S}(m \mid s \gg \text{Kfor } s; k@P) \longrightarrow \mathcal{S}(m \mid s_1 \gg \text{KforPost Sfor}(\text{Sskip}; e; s_1) \text{ do } s_2 \text{ join } L; k@P)} \\
\frac{s = \text{Sfor}(\text{Sskip}; e; s_1) \text{ do } s_2 \text{ join } L}{\mathcal{S}(m \mid \text{Sbreak} \gg \text{Kfor } s; k@P) \longrightarrow \mathcal{S}(m \mid \text{Sskip} \gg k@P)} \\
\frac{s = \text{Sfor}(\text{Sskip}; e; s_1) \text{ do } s_2 \text{ join } L}{\mathcal{S}(m \mid \text{Sskip} \gg \text{KforPost } s; k@P) \longrightarrow \mathcal{S}(m \mid s \gg k@P)}
\end{array}$$

B.4 Expression Rules

$$\begin{array}{c}
\mathcal{P}', pt, \boxed{vt, \bar{lt}} \leftarrow \text{MallocT}(\mathcal{P}, vt) \quad m', p \leftarrow \text{heap_alloc size } m \\
\frac{m'' = m' [p + i \mapsto (\text{undef}, vt, lt) \mid 0 \leq i < s]}{\mathcal{E}(m \mid \text{ctx} [\text{malloc}(\text{size}@t)] \gg k@P) \longrightarrow \mathcal{E}(m'' \mid \text{ctx} [\text{Eval } p@pt] \gg k@P')} \\
\frac{m[l]_{|ty|} = v@vt@l\bar{t} \quad vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \bar{lt})}{\mathcal{E}(m \mid \text{ctx} [\text{EvalOf Eloc } l@pt] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [\text{Eval } v@vt'] \gg k@P)} \\
\frac{m[l]_{|ty|} = v_1@vt@l\bar{t} \quad \oplus \in \{+, -, *, /, \%, <, >, \&, ^, |\}}{vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \bar{lt}) \quad e = \text{Eassign Eloc } l@pt \text{ Ebinop } \oplus \text{ Eval } v_1@vt' \text{ Eval } v_2@vt_2} \\
\frac{\mathcal{E}(m \mid \text{ctx} [\text{EassignOp } \oplus \text{ Eloc } l@pt \text{ Eval } v_2@vt_2] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [e] \gg k@P)} \\
\frac{m[l] = v@vt@l\bar{t} \quad \oplus \in \{+, -\} \quad vt' \leftarrow \text{LoadT}(\mathcal{P}, pt, vt, \bar{lt})}{vt \leftarrow \text{ConstT } e = \text{Ecomma Eassign Eloc } l@pt \text{ Ebinop } \oplus \text{ Eval } v@vt' \text{ 1@ConstT Eval } v@vt'} \\
\frac{\mathcal{E}(m \mid \text{ctx} [\text{EpostInc } \oplus \text{ Eloc } l@pt] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [e] \gg k@P)} \\
\frac{m[l]_{|ty|} = v_1@vt_1@l\bar{t} \quad m' = m[l \mapsto v_2@vt'@l\bar{t}']}{\mathcal{P}', vt', \bar{lt}' \leftarrow \text{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \bar{lt})} \\
\frac{\mathcal{E}(m \mid \text{ctx} [\text{Eassign Eloc } l@pt \text{ Eval } v_2@vt_2] \gg k@P) \longrightarrow \mathcal{E}(m' \mid \text{ctx} [\text{Eval } v_2@vt_2] \gg k@P')} \\
\frac{le[id] = (l, _, pt, ty) \quad pt \leftarrow \text{VarT}(\mathcal{P}, vt)}{\mathcal{E}(m \mid \text{ctx} [\text{Evar } id] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [\text{Eloc } l@pt] \gg k@P)} \\
\frac{\langle \odot \rangle v = v' \quad vt' = \text{UnopT}(\mathcal{P}, vt) \mathcal{P} vt}{\mathcal{E}(m \mid \text{ctx} [\text{Eunop } \odot \text{ Eval } v@vt] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [\text{Eval } v'@vt'] \gg k@P)} \\
\frac{v_1 \langle \oplus \rangle v_2 = v' \quad vt' = \text{BinopT}(\mathcal{P}, vt_1, vt_2) \mathcal{P} vt_1 vt_2}{\mathcal{E}(m \mid \text{ctx} [\text{Ebinop } \oplus \text{ Eval } v_1@vt_1 \text{ Eval } v_2@vt_2] \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [\text{Eval } v'@vt'] \gg k@P)} \\
\frac{}{\mathcal{E}(m \mid \text{ctx} [\text{Ecall } f' \overline{v@vt}] \gg ty@P) k \longrightarrow C(f', m, ge \mid le(v@vt) \gg \text{Kcall } f \text{ ctx } [] k@P)}
\end{array}$$

B.5 Call and Return Rules

$$\begin{array}{c}
\text{def}(f) = (xs, s) \\
\frac{le' = le[x \mapsto v@vt' \mid (x, v@vt) \leftarrow \text{zip}(xs, args), vt' \leftarrow \text{ArgT}(\mathcal{P}, vt, f, x)]}{C(f, m, ge \mid le(args) \gg k@P) \longrightarrow \mathcal{S}(m \mid ge \gg le'@P) sk} \\
\frac{k = \text{Kcall } le' \text{ ctx } k' \quad \mathcal{P}'', vt' \leftarrow \text{CallerRetT}(\mathcal{P}, \mathcal{P}', vt)}{\mathcal{R}(m, ge, le \mid \text{Eval } v@vt \gg k@P) \longrightarrow \mathcal{E}(m \mid \text{ctx} [\text{Eval } v@vt'] \gg k'@P')}
\end{array}$$